Defense Information Infrastructure (DII)

Common Operating Environment (COE)

Consolidated System Administrator’s Guide Version 3.0 (HP and Solaris)

3 January 1997

Prepared for:

Defense Information Systems Agency

Table of Contents

Table of Contents (continued)

Table of Contents (continued)

Table of Contents (continued)

List of Tables

Part 1:

List of Figures

Part 1:

Table of Contents (continued)

Part 2:

This page intentionally left blank.

Forward

The DII COE Consolidated System Administrator's Guide is part of a set of DII COE developer documentation published in conjunction with major or general releases of the DII COE (such as DII COE Version 3.0). It contains the latest information available on the date of release of this publication.

NOTE: Contact the Defense Information Systems Agency (DISA) for information concerning the Commercial-Off-The-Shelf (COTS) licensed software and supporting documentation.

Segment Availability: The information contained herein may precede the availability of certain DII COE software segments. Please visit the DISA's DII COE Home Page on the World Wide Web to obtain the most current information available and to obtain the latest available release of DII COE software segments and other related documentation required by your organization.

DISA DII COE Home Page URL:	**http://www.disa.mil/dii/diicoe or** **http://204.34.175.79/dii/**

Segment Documentation Applicability: Software segments and the asociated documentation are identified by their DII COE segment release version number and/or product version number, as available. It is important to note, however, that documentation released with a given segment version may be applicable to subsequent version(s) of the same software segment. For example, the installation guide for a DII segment version 3.0.0.3 may also apply to version 3.0.0.4 of the same segment unless superseded by a new release of the documentation. Refer to the details provided in the Version Description Document (VDD) for a particular segment release and its related amendments or errata to obtain the most current information on the fixes incorporated, additional sources of information, or reference documents.

This page intentionally left blank.

Part 1. System Administrator's Guide for HP and Solaris Version 3.0.0.3

Preface

The following conventions have been used in this document:

[HELVETICA FONT]	Used to indicate keys to be pressed. For example, press [RETURN].
`Courier Font`	Used to indicate entries to be typed at the keyboard, UNIX commands, titles of windows and dialog boxes, file and directory names, and screen text. For example, execute the following command: `tar xvf /dev/rmt/3mn`
"Quotation Marks"	Used to indicate prompts and messages that appear on the screen.
Italics	Used for emphasis.

This page intentionally left blank.

1. Introduction

This document describes general information about the Defense Information Infrastructure (DII) Common Operating Environment (COE) and the system administration utilities of the DII COE kernel.

This guide is divided into eight sections and three appendices:

Section/Appendix	Page
Introduction Provides a high-level overview of the DII COE and provides a list of additional sources of information.	3
DII COE Environment Lists hardware components and kernel components.	7
Operating Guidelines Explains startup and shutdown of the software and the hardware.	9
DII COE Kernel and Segment Installation Overview Provides instructions for performing local, remote, and network installations of the DII COE kernel and software segments.	11
Common Desktop Environment Provides information about using the Common Desktop Environment (CDE) to provide a standard environment for managing applications and functions.	13
System Administration Utilities Describes DII COE maintenance and management functions available to a system administrator.	21
Security Administration Command Line Utilities Describes how to change the security level of a workstation and enable or disable auditing.	61
Error Recovery Guidelines Describes potential problems, errors, and solutions.	65
Communications Provides information about networks, physical interfaces to the system, communications and broadcast configuration, and troubleshooting.	69
Multiple Monitor and Keyboard Configurations Shows recommended single-eye and dual-eye configuration schemes.	79
Database Size Limits Lists database limits for various DII COE files.	81

1.1 The DII COE Kernel

The DII COE kernel consists of the DII COE software required on every workstation. The kernel provides the commercial software of X Windows, Motif, and UNIX, as well as the DII COE System Administration, Security Administration, and runtime environment software. Figure 1 shows a graphical representation of the DII COE kernel and the segment installation process.

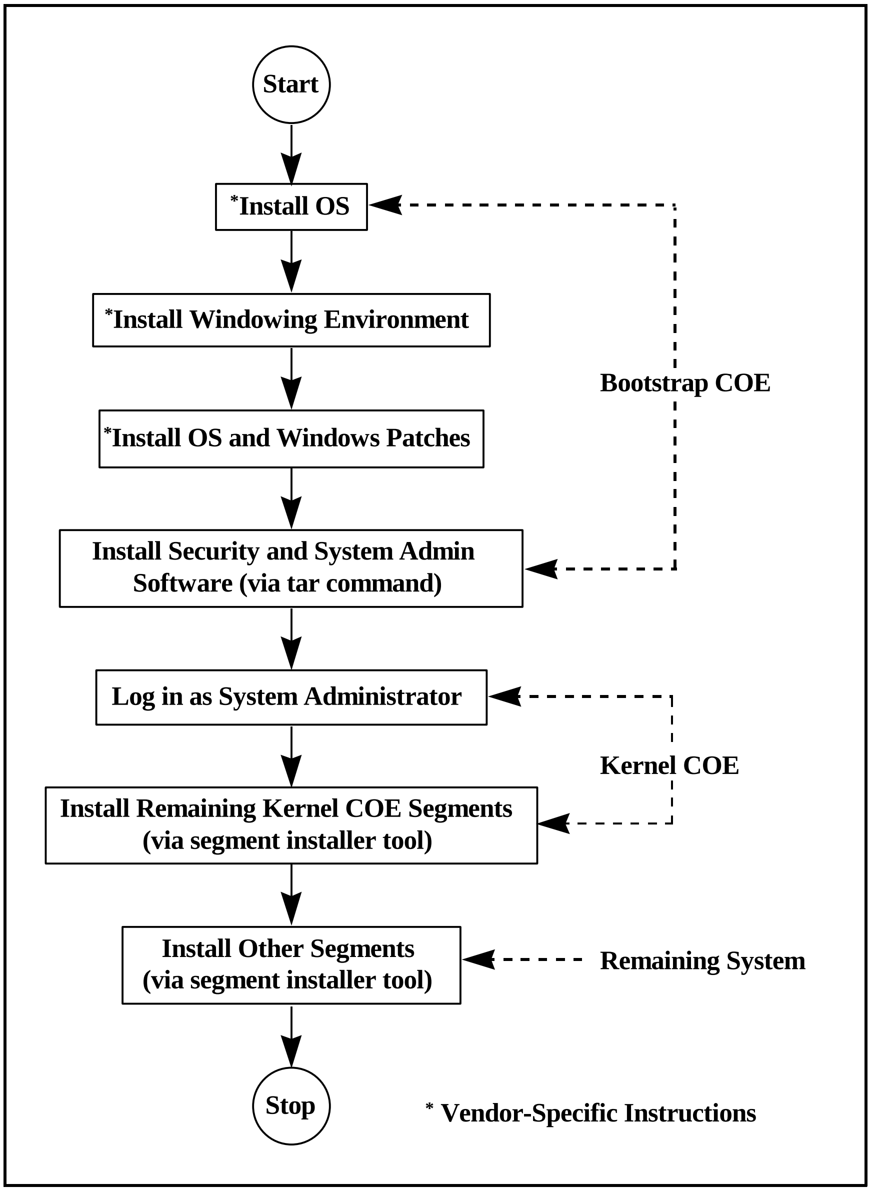

Start
*Install OS
*Install Windowing Environment
*Install OS and Windows Patches
Install Security and System Admin Software (via tar command)
Bootstrap COE
Log in as System Administrator
Install Remaining Kernel COE Segments (via segment installer tool)
Kernel COE
Install Other Segments (via segment installer tool)
Remaining System
Stop
* Vendor-Specific Instructions

Figure 1. DII COE Kernel and Segment Installation

Refer to the *DII COE Kernel Installation Guide (HP-UX 9.07)*, *DII COE Kernel Installation Guide (Solaris 2.4)*, and *DII COE Kernel Installation Guide (Solaris 2.5.1)* for more information about installing the DII COE kernel and segments.

1.2 Additional Sources of Information

Reference the following documents for more information about the DII COE and about CDE:

Defense Information Infrastructure (DII) Common Operating Environment (COE) Integration and Runtime Specification Version 2.0, DII COE I&RTS:Rev 2.0, Inter-National Research Institute, October 23, 1995

- *Defense Information Infrastructure (DII) Common Operating Environment (COE) Kernel Installation Guide (HP-UX 9.07) FINAL* Version 3.0.0.3, DII.3003.Final.HP907.IG-1, Inter-National Research Institute, October 29, 1996
- *Defense Information Infrastructure (DII) Common Operating Environment (COE) Kernel Installation Guide (Solaris 2.4) FINAL* Version 3.0.0.3, DII.3003.Final.Sol24.IG-1, Inter-National Research Institute, October 29, 1996
- *Defense Information Infrastructure (DII) Common Operating Environment (COE) Kernel Installation Guide (Solaris 2.5.1) FINAL* Version 3.0.0.3, DII.3003.Final.Sol251.IG-1, Inter-National Research Institute, October 29, 1996
- *Triteal Enterprise Desktop 4.0 User's Guide*, Triteal Corporation, 1995.

2. DII COE Environment

This section describes DII COE hardware components and DII COE kernel components.

Supported UNIX host computers for the current DII COE are:

- HP
- Sun SPARC.

2.1 Hardware Components

The software may reside on a single disk or across multiple disks.

2.1.1 HP Hardware

- HP 9000/7xx, with at least 64 megabytes (MB) of random access memory (RAM)
- Hard disk drive [at least 1.2 gigabytes (GB) or larger].

2.1.2 Sun SPARC Hardware

- Sun SPARC with at least 64MB of RAM

C Hard disk drive (at least 1.2GB or larger).

2.2 Kernel Components

The DII COE kernel is a suite of applications layered on top of the HP-UX or Solaris operating system. The DII COE kernel media contains software relating to several areas:

C Operating system

C System and Security Administration software

C X Windows system software

C Motif system software

C CDE

C Distributed Computing Environment (DCE).

3. Operating Guidelines

This section provides operating guidelines for powering up and powering down the system.

3.1 Power Down

NOTE: Never power down the system without first executing a shutdown, as described in the steps below. Doing so could cause irreparable damage.

STEP 1: **Log in**. Log in with a sysadmin account and password at the prompts.

STEP 2: **Shut down the machine**. Select the `Shutdown` option from the `Hardware` pull-down menu and respond to the appropriate prompts.

STEP 3: **Wait until the system is fully down**.

STEP 4: **Turn off the peripherals**. Turn off the peripherals, including the monitor.

STEP 5: **Turn off the computer**.

3.2 Power Up

STEP 1: **Turn on the Uninterruptable Power Supply (UPS)**. Turn on the UPS if necessary.

STEP 2: **Turn on the peripherals**. Turn on the peripherals, including the monitor.

STEP 3: **Turn on the computer**.

STEP 4: **Log in**. Log in with your assigned account and password at the prompts.

4. DII COE Kernel and Segment Installation Overview

This section provides an overview of installation procedures for the DII COE kernel tape and one or more application segment tapes (e.g., Netscape).

NOTE: Applications are designed to run with specific operating systems. Before installing any operating system or any segment, make sure the tape you are loading is the correct one. This can be verified by checking the label on the tape.

NOTE: The DII COE is installed using an automated installation procedure that removes previously installed software and overwrites existing data files. This type of installation is called a *destructive installation*. Therefore, it is advised that you back up any data you want to save before beginning any installation procedure.

4.1 Installing the Operating System and Kernel

Reference the *DII COE Kernel Installation Guide (Solaris 2.4)*, the *DII COE Kernel Installation Guide (Solaris 2.5.1)*, and the *DII COE Kernel Installation Guide (HP-UX 9.07)* for details on installing the operating system and kernel for the respective system.

4.2 Installing Segments

Installation of the DII COE and DII COE segments varies depending on the hardware architecture, the processor, and the type or number of segments being loaded.

Segments may be loaded or installed from tape drive or from hard disk. The source can be local, remote, or network:

- Local—from a tape drive physically attached to the machine
- Remote—from a tape drive physically attached to another machine
- Network—from a segment installation server attached to the local area network (LAN).

4.2.1 Local Installation

To install DII COE segments locally, use the segment tapes and a tape drive attached to the machine being installed. The tape drive and the distribution medium must be compatible. For example, a 4mm DAT drive cannot be used to load or install an application delivered on a cartridge tape. Installing from a local source is convenient because it does not rely on a network to reach another machine. Refer to Section 6.3.1, *Segment Installer Option*, for more information about installing segments.

4.2.2 Remote Installation

To install DII COE segments from a remote source, the machine being loaded must have network capability. In addition, you need to know the remote machine's system name or IP address. A remote source is used when a local tape drive is unavailable or when the tape drive on the machine being installed is incompatible with the tapes. For example, an HP segment can be loaded or installed from an HP workstation or from a Sun SPARCstation. Refer to Section 6.3.1, *Segment Installer Option*, for more information about installing segments.

4.2.3 Network Installation

To install DII COE segments from a network source, the segments must first be loaded onto one or more segment servers (the hard disk of one or more network machines). Loading a segment is different than installing a segment. Loading a segment on a machine stores the segment on the machine, but does not enable the segment to run. Instead, segments stored on a segment installation server are available for installation without the installation medium because they are located on a server. Segments can, then, be installed individually on each machine on the network. However, network installations require the system to be configured with networking capabilities. Refer to Section 6.3.2, *Segment Installation Server Option*, for more information about loading segments on a segment installation server.

NOTE: Loading segments on multiple machines is highly recommended because it ensures easy access to the software and does not require the user to locate segment installation tapes.

5. Common Desktop Environment

The DII COE kernel is a suite of applications layered on top of the HP-UX or Solaris Operating System. The Common Desktop Environment (CDE) is one of several software programs that comprise the kernel. CDE provides a standard environment for managing applications and functions within one or more workspaces. To help organize your desktop, you can place special applications in a particular workspace and name that workspace accordingly.

The CDE has a horizontal window at the bottom of the display called a Front Panel, which is a desktop window that exists in all workspaces. The CDE remains open as different workspaces are opened. Figure 2 shows a CDE Front Panel. The panel below includes the following icons: Clock, Calendar, File Manager, Text Editor, Mailer, Workspace Switch, lock, Graphical Workspace Manager (GWM), EXIT, Default Printer, Style Manager, Application Manager, Help Manager, and Trash Can. These icons are controls and indicators for completing tasks. The controls and indicators shown in Figure 2 are described in greater detail in the following subsections.

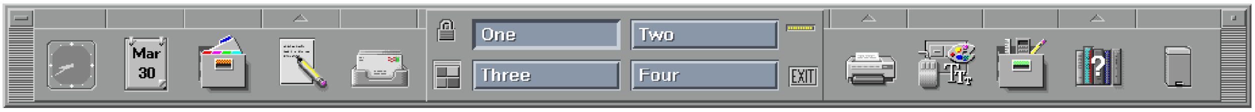


Figure 2. CDE Front Panel

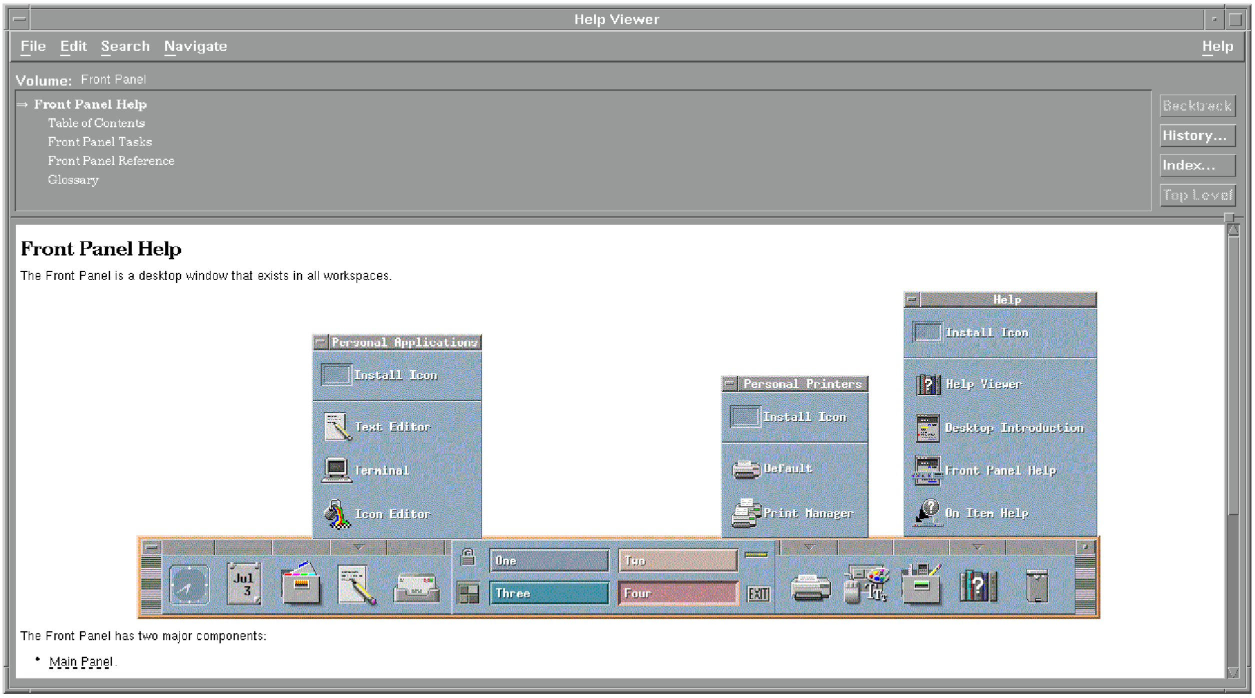
5.1 Subpanels

The default Front Panel contains subpanels. Controls with subpanels have a button with an upward arrow above them. This button is used to display or close the subpanel. For example, the Text Editor—Personal Applications, Personal Printers, and Help Manager controls have subpanels (Figure 3). Subpanels contain an `Install Icon` control, which allows the user or system administrator to customize the Front Panel, an icon that will start the application, and other controls. Dropping a file, folder, or action icon on the `Install Icon` control installs the file, folder, or action item in that subpanel.

To open a subpanel, click the arrow button above the control. To close a subpanel, click the down arrow that appears at the bottom of the subpanel.

NOTE: If you have not moved a subpanel from its initial position, it closes automatically when you choose a control.

Initially, the Text Editor—Personal Applications, Personal Printers, and Help Manager controls have subpanels. In addition, you can add subpanels to other controls. The CDE can be customized: Your front panel may contain additional subpanels, and the subpanels may contain additional or different controls. In other words, you can add controls to subpanels, interchange Front and subpanel controls, add subpanels, add or delete workspaces, or rename workspaces.



Volume: Front Panel

⇒ Front Panel Help
Table of Contents
Front Panel Tasks
Front Panel Reference
Glossary

Front Panel Help

The Front Panel is a desktop window that exists in all workspaces.

The Front Panel has two major components:

- Main Panel

Figure 3. CDE Subpanels

5.1.1 Adding and Removing Subpanels

Follow the steps below to add or remove a subpanel.

STEP 1: **Indicate which subpanel should be added or removed**. Point to the control in the front panel whose subpanel you want to add or remove.

STEP 2: **Add or remove the subpanel**. Choose `Add Subpanel` or `Delete Subpanel` from the control’s pop-up menu (see subsection 5.3, *Pop-up Menus*, for more information about pop-up menus).

5.1.2 Moving a Subpanel

Follow the steps below to move a subpanel.

STEP 1: **Indicate which subpanel should be moved**. Point to the subpanel’s window frame.

STEP 2: **Move the subpanel**. Hold down the left mouse button as you drag the subpanel to its new location.

5.2 Controls and Indicators

The CDE contains controls and indicators. A control, when selected, allows the user to access applications and utilities. The Calendar, File Manager, Mailer, Workspace Switch, Lock, Graphical Workspace Manager (GWM), Exit, Printer, Style Manager, Application Manager, Help Manager, and Trash Can are examples of controls. An indicator does not have a specific action when selected—it simply provides information. The Clock and the Busy Light are two examples of indicators.

The default indicators and controls that comprise the CDE are described in the following subsections as they appear from left to right on the CDE front panel. Since it can be customized, your Front Panel may contain additional or different controls. Reference the *Triteal Enterprise Desktop 4.0 User's Guide* for additional information on the CDE.

5.2.1 Clock

The Clock is an indicator that displays the current time, which is maintained by the operating system.

5.2.2 Calendar

The Calendar is a control that displays the system date. Click on the Calendar to start the Calendar application. The Calendar application enables scheduling of appointments and creation of To Do lists. Day, week, month, and year calendar views are available. Appointments can be scheduled, deleted, and listed.

5.2.3 File Manager

The File Manager control opens a view of your home folder or of a selected folder. This application is used to manage the files and directories of a system, as well as to create, edit, rename, and delete files and folders. Click on the File Manager control to open a view of your home folder, or drop a file on the File Manager control to open a view of the dropped folder.

5.2.4 Text Editor—Personal Applications

The Text Editor**—**Personal Applications control is used to edit text. Click on the Text Editor control to start the desktop Text Editor application. Dropping a file on the Text Editor control opens the file in a new Text Editor window.

This control position is reserved for a personal application of your choice. To place an application other than the Text Editor in this control position, install the new application icon into the Personal Applications subpanel. Applications are installed from the Application Manager (see Section 5.2.13, *Application Manager*) by dragging the icon from the Application Manager window to the Install Icon control. Once the application is installed in the Personal Applications subpanel, you can use the control’s pop-up menu to place that control in the Front Panel.

NOTE: These icons may not function based on profile selection.

Using this same installation process, you can store frequently used applications in the Personal Applications subpanel, such as the Terminal control, and the Icon Editor control. These two controls are discussed in the following subsections.

5.2.4.1 Terminal

The Terminal control is used to open a terminal emulator window. Click on the Terminal control to open the window.

NOTE: For security reasons, this option has been removed from the CDE Front Panel for all users except root. Root users can access the Terminal control from the Text Editor**—**Personal Applications control subpanel.

If you are logged in with a System Administration account and want to access a terminal emulator window, follow the steps below:

STEP 1: Double-click on the Application Manager control on the CDE Front Panel to open the `Application Manager` window.

STEP 2: Double-click on the `DII_APPS` folder in the `Application Manager` window to open the `Application Manager - DII_APPS`folder.

STEP 3: Double-click on the `SA_Default` folder to open the `Application Manager - SA_Default` window. This window contains both a `Dtterm` icon and an `Xterm` icon.

STEP 4: Double-click on either the `Dtterm` icon or the `Xterm` icon to open the window.

5.2.4.2 Icon Editor

The Icon Editor control is used to create new icons (bitmap and pixmap files) or edit existing icons. Click on the Icon Editor control to open the Icon Editor application.

5.2.5 Mailer

The Mailer control is used to create, send, and receive electronic messages and attachment files. Click on the Mailer control to start the Mailer application. To mail one or more files, select the file(s) in File Manager, drag the file(s) from File Manager and drop them on the Mailer control, type the subject and destination address(es) into the `New Message` dialog box, and click on the `Send` button.

The Mailer control includes an indicator, which indicates the arrival of new mail. Dropping a file on the Mailer control opens the file's contents in the Mailer's New Message window.

5.2.6 Workspace Switch

The Workspace Switch allows you to change workspaces. To help organize your desktop, you can place special applications in a particular workspace and name that workspace accordingly. Each workspace, therefore, contains only those applications and functions you want to group together. The Workspace Switch is located in the center of the CDE Front panel. It contains buttons with the words "`One`", "`Two`", "`Three`", and "`Four`", which are controls used to select one of four workspaces. The button for the current workspace is "pushed in" (i.e., inset from the other three). To change the name of the current workspace, click its button and edit the name in the button.

5.2.7 Lock Control

The Lock icon locks the display and keyboard, thereby preventing unauthorized input. No input from your keyboard or mouse will be allowed until you unlock the display with your password. Click on the Lock control to lock the display.

5.2.8 GWM Control

The GWM control is used to start the Graphical Workspace Manager (GWM), which provides a visual representation of the application windows available in all of the workspaces. The GWM is used to control the size, placement, and operation of windows within multiple workspaces, as well as maintain a depiction of the windows as the user creates, moves, and otherwise manipulates them. Click on the GWM control to start the GWM application.

5.2.9 Busy Light Indicator

The Busy Light indicator blinks to indicate that the system is running an action.

5.2.10 EXIT Control

The EXIT control is used to log out of the desktop and end the desktop session. Click on the EXIT control to end the current session.

5.2.11 Personal Printers

The Personal Printers control displays the status of the default printer and allows cancellation of print jobs on that printer. Click on the Printer control to open the Printer Jobs dialog box, which shows the status of print jobs on the default printer. Drag a file from the Application Manager of the File Manager and then drop them onto the Printer control to print them on the default printer.

The Personal Printers subpanel contains the following applications: Install Icon, Default Printer, and Print Manager. Install Icon is used to install an icon dragged from File Manager or Application Manager onto the subpanel. Print Manager is used to print a file on the default printer.

5.2.12 Style Manager

The Style Manager is used to customize the appearance and behavior of your desktop session. Specifically, the Style Manager control allows customization of the backdrop, keyboard, screen, fonts, colors, mouse, startup, beep, and window. Click on the Style Manager control to start the Style Manager application. If the application is already running, its window is raised to the top of the window stack.

5.2.13 Application Manager

The Application Manager is a container for the applications registered on your system. Click on the Application Manager control to open an `Application Manager` window. This window contains folders of application groups, such as tools and applications. These folders contain icons that, when selected, start applications.

5.2.14 Help Manager

The Help Manager control lists information about CDE topics. Click on the Help Manager control to open a `Help View` window displaying the top level of help information. The help available on your system is organized hierarchically. The top level lists all the help “families” on your system. When you click on a family to open it, you will see a list of all the help “volumes” in that family. The Index feature in the `Help View` window is used to search for topics.

The Help Manager subpanel contains the following applications: Desktop Introduction, which provides an introduction to the desktop; Front Panel Help, which provides an introduction to the front panel of the CDE; and On-Item Help, which provides information on a selected control.

5.2.15 Trash Can

The Trash Can stores files for deletion. Click on the Trash Can control to open the `Trash Can` window. Dropping a file or folder on the Trash Can control moves the file or folder to the Trash Can. The Trash Can is emptied by opening the Trash Can, selecting files to be deleted, choosing `Shred` from the `File` menu or from the `Trash Can` pop-up menu, and then clicking `OK` in the confirmation window.

5.3 Pop-up Menus

CDE Front Panel controls include pop-up menus. The contents of a control’s pop-up menu depends on the behavior of the control and its location. To display a Front Panel pop-up menu, point to the control and press the right mouse button.

5.3.1 Pop-up Menus for Front Panel Controls

If the control starts an application, the first entry in the menu is a command that starts the application. Choosing the menu option has the same effect as clicking on the control. If the Front Panel control does not have a subpanel, clicking on the control with the right mouse button will display the following pop-up menu options: `[Name of the control]`, `Add Subpanel`, and `Help`.

`[Name of the control]`
Starts the application (if the control starts an application).

`Add Subpanel`
Adds a subpanel to the control.

`Help`
Displays on-line help for the control.

5.3.2 Pop-up Menus for Front Panel Controls with Subpanels

If the Front Panel control has a subpanel, clicking on the control with the right mouse button will display the following pop- up menu: `[Name of the control]`, `Remove Subpanel`, and `Help`.

`[Name of the control]`
Starts the application (if the control starts an application).

`Remove Subpanel`
Removes the subpanel and its contents.

`Help`
Displays on-line help for the control.

5.3.3 Pop-up Menu for the Switch Area

The switch area is the portion of the workspace switch not occupied by other controls or workspace buttons. The pop-up menu contains the following options: `Add Workspace` and `Help`.

`Add Workspace`
Adds a workspace.

`Help`
Displays help for the workspace switch.

5.3.4 Pop-up Menu for Workspace Buttons

Workspace buttons are used to change workspaces. Each button has its own menu, which contains the following options: `Add Workspace`, `Delete`, `Rename`, and `Help`.

`Add Workspace`
Adds a workspace.

`Delete`
Deletes the workspace.

`Rename`
Turns the button label into a text field for editing the name.

`Help`
Displays help for the workspace switch buttons.

5.3.5 Pop-up Menu for Subpanel Controls

The pop-up menu for subpanel controls includes a command for making a particular control the current Front Panel control. The pop-up menu contains the following options: `Copy to Main Panel`, `Remove`, and `Help`.

`Copy to Main Panel`
Duplicates the control in the Front Panel, replacing the current Front Panel control.

`Remove`
Removes the control from the subpanel.

`Help`
Displays on-line help for the control.

6. System Administration Utilities

This section describes the DII COE System Administration application, which provides options for DII COE maintenance and management. To access utilities, log in with a system administration user account.

Options are grouped according to their functionality and are located on pull-down menus or as icons within the application manager. Some options may have a cascading menu. Availability of specific menu options depends on two criteria:

- C Hardware type (e.g., HP or SPARC)

- C Access assigned to the user account profile.

The System Administration application has the following pull-down menus: `SA System`, `Hardware`, `Software`, and `Network`. In addition, one system administration task may be performed from the command line: removing global data. These system administration utilities are described in the following sections.

6.1 SA System Menu

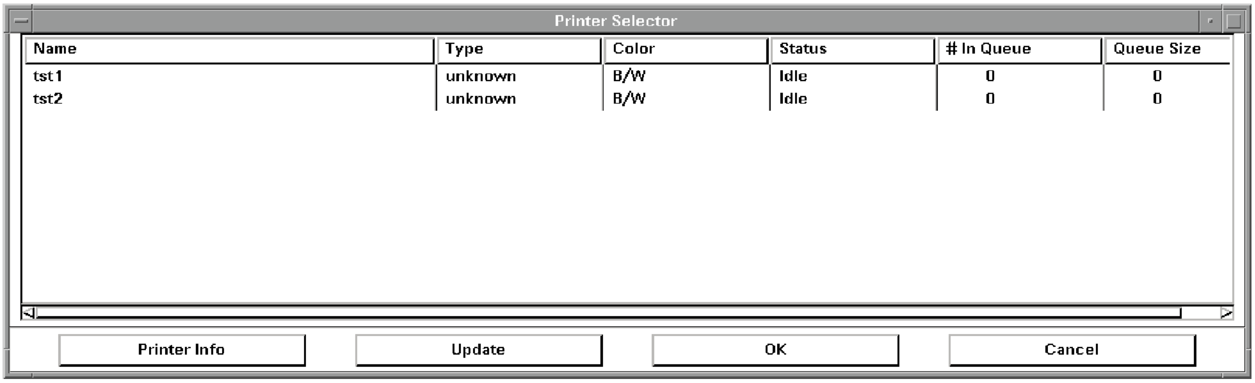
The `SA System` menu contains the following options: `Printer` and `Close All`. These options are described in the subsections below.

6.1.1 Printer Option

The `Printer` option is used to select a default printer and to view print jobs stored in the local queue. The `Printer` option has a cascading menu that contains two options: `Printer Select` and `Print Jobs`.

6.1.1.1 Printer Select Option

The `Printer Select` option is used to select a default printer. After selecting the `Printer Select` option, the `Printer Selector` window appears (Figure 4). The window shows all printer selections. The default printer will be highlighted. To change the default printer, click on a different printer to highlight it and click on the `OK` button.



Name	Type	Color	Status	# In Queue	Queue Size
tst1	unknown	B/W	Idle	0	0
tst2	unknown	B/W	Idle	0	0

Figure 4. Printer Selector Window

Printer Selector Window Fields

The `Printer Selector` window has the following fields: `Name`, `Type`, `Color`, `Status`, `# In Queue`, and `Queue Size`. These fields are described below.

`Name`
Lists printer names. The printer selections listed in this field are selected using the Admintool for Solaris and SAM (system administration manager tool) for HP. Admintool and SAM are located in the `Application Manager - SA_Default` window. To access this window, double-click on the Application Manager control on the CDE Front Panel to open the `Application Manager` window, double-click on the `DII_APPS` folder in the `Application Manager` window to open the `Application Manager - DII_APPS`folder, and double-click on the `SA_Default` folder to open the `Application Manager - SA_Default` window.

NOTE: Refer to vendor documentation for information on using SAM and Admintool to add printers to the `Printer Selector` window.

`Type`
Shows the printer type.

`Color`
Shows the viewing option (color or black and white).

`Status`
Shows the status of the printer. Sample statuses are `Idle` (printer is currently idle), `Busy` (printer is currently processing jobs), `Error` (printer has detected an error), and `Unknown` (unable to determine the printer status).

`# In Queue`
Shows the number of print jobs in the print queue.

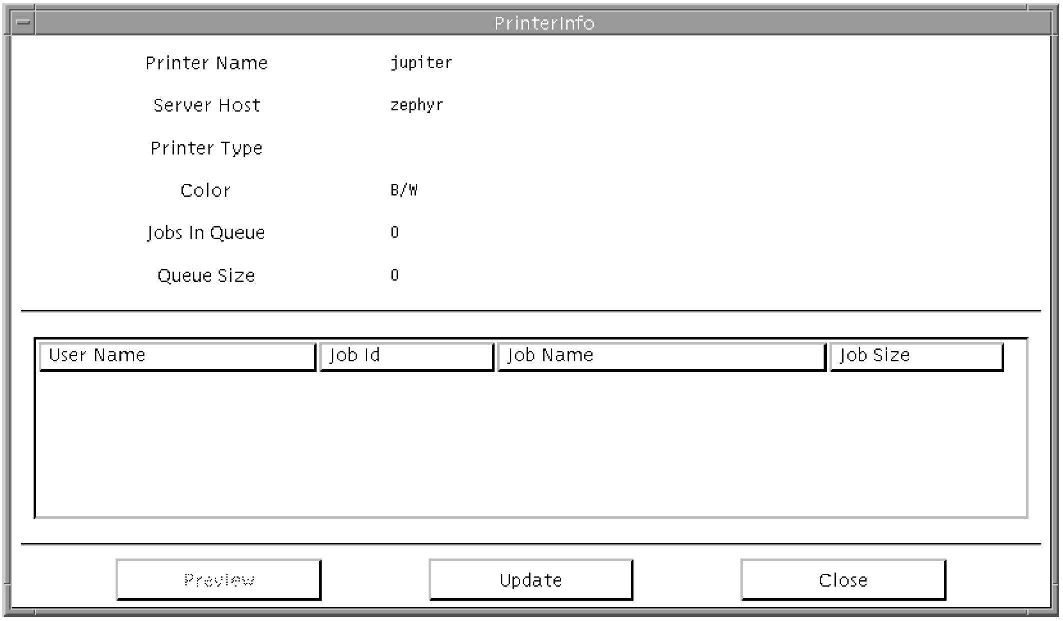
`Queue Size`
Shows the total size of all jobs in the queue.

Printer Selector Window Buttons

The `Printer Selector` window has the following buttons: `Printer Info`, `Update`, `OK`, and `Cancel`. These buttons are described below.

`Printer Info`

Used to show information about each printer selection listed in the `Printer Selector` window. To show information about print jobs queued to a specific printer listed in the `Printer Selector` window, click on a printer to highlight it and click on the `Printer Info` button. The `PrinterInfo` window appears (Figure 5). This window shows the printer name, server host, printer type, color (e.g., color or black and white), number of jobs in the queue, and queue size for the selected printer. It also shows the user name of the person who sent each print job to the selected printer, each job ID, each job name, and each job size.



Printer Name	jupiter
Server Host	zephyr
Printer Type	
Color	B/W
Jobs In Queue	0
Queue Size	0

User Name	Job Id	Job Name	Job Size

Figure 5. PrinterInfo Window

`Update`

Used to update entries on the `Printer Selector` window.

`OK`

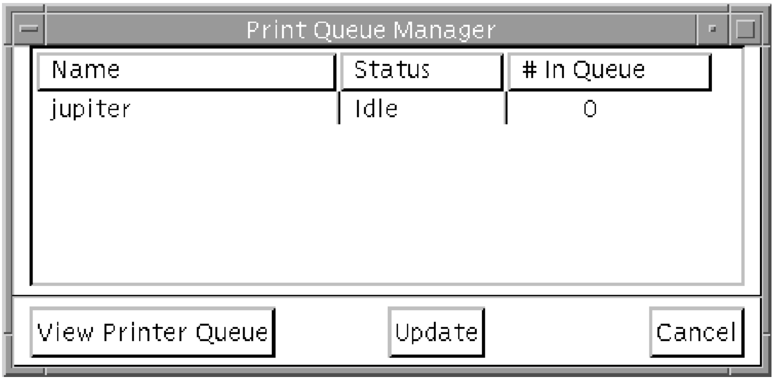
Used to save any changes made to the default printer.

`Cancel`

Used to close the `Printer Selector` window.

6.1.1.2 Print Jobs Option

The `Print Jobs` option is used to allow the user to view the print jobs stored in the local queue. After selecting the `Print Jobs` option, the `Print Queue Manager` window appears (Figure 6).



Name	Status	# In Queue
jupiter	Idle	0

Figure 6. Print Queue Manager Window

Print Queue Manager Fields

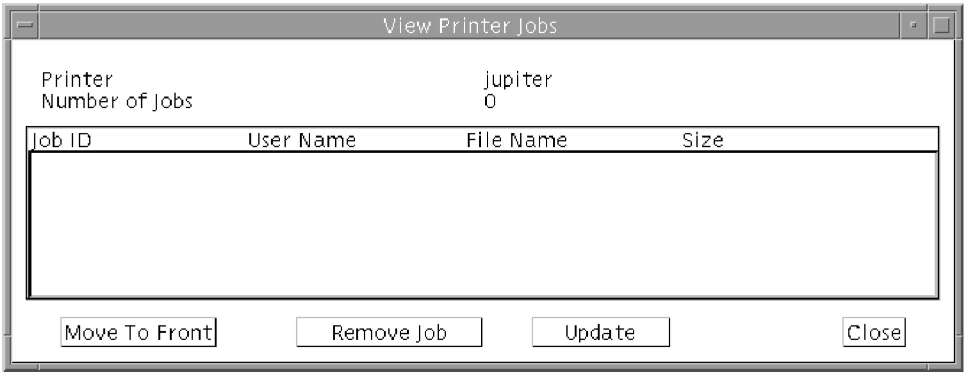
The `Print Queue Manager` window has the following fields: `Name`, `Status`, and `# In Queue`. These fields are described below.

`Name`
Shows the printers supported on the system.

`Status`
Shows the status of the printer (e.g., `Idle`, `Busy`, `Error`, `Unknown`).

`# In Queue`
Shows the number of print jobs in the print queue.

To show the print jobs for a specific printer listed in the `Print Queue Manager` window, click on a printer in the list to highlight it and click on the `View Printer Queue` button. The `View Printer Queue` button is used to provide information about print jobs in the local queue. The `View Printer Jobs` window appears (Figure 7).



Printer jupiter
Number of Jobs 0

Job ID	User Name	File Name	Size

Figure 7. View Printer Jobs Window

View Printer Jobs Window Fields

The `View Printer Jobs` window has the following fields: `Job ID`, `User Name`, `File Name`, and `Size`. These fields are described below.

`Job ID`
Shows the ID number automatically assigned by the system.

`User Name`
Shows the name of the user who sent the job to the printer.

`File Name`
Shows the name of the file sent to the printer.

`Size`
Shows the size of the print file in bytes.

View Printer Jobs Window Buttons

The `View Printer Jobs` window has the following buttons: `Move To Front`, `Remove Job`, `Update`, and `Close`. These buttons are described below.

`Move To Front`
Used to change the priority of a selected print job in the printer queue. To move a print job to the front of the queue, click on the print job in the `View Printer Jobs` window to highlight it and click on the `Move To Front` button.

`Remove Job`
Used to remove a print job from the printer queue. To remove a print job, click on the print job in the `View Printer Jobs` window to highlight it and click on the `Remove Job` button.

`Update`
Used to update entries in the `View Printer Jobs` window.

`Close`
Used to close the `View Printer Jobs` window and return to the `Print Queue Manager` window.

6.1.2 Close All Option

The `Close All` option is used to close all the windows launched from the menu bar or from the `DII_APPS` folder. To access the `DII_APPS` folder, double-click on the Application Manager control on the CDE Front Panel to open the `Application Manager` window. The `DII_APPS` folder is located in this window.

NOTE: The `Close All` option does not close windows opened from the CDE front panel. Refer to Section 5, *Common Desktop Environment*, for more information about CDE.

6.2 Hardware Menu

The `Hardware` menu contains the following options: `Shutdown System`, `Reboot System`, and `Disk Manager`. These options are described in the following subsections.

6.2.1 Shutdown System Option

The `Shutdown System` option is used to shut down the system safely before powering down the machine.

NOTE: Never power down the system without first executing a shutdown, as described in the steps below. Doing so could cause irreparable damage.

Follow the steps below to shutdown the system.

STEP 1: **Select the `Shutdown System` option**. The `Shutdown` dialog box appears with the following message: `Do you want to shutdown the computer?`

STEP 2: **Shut down the system**. Click on the `OK` button to continue the shutdown process.

STEP 3: **Turn off the system**. Turn off the machine when the system is completely down. System messages appear that indicate the system is ready to power down.

6.2.2 Reboot System Option

The `Reboot System` option is used to reboot the system. Follow the steps below to reboot the system.

STEP 1: **Select the `Reboot System` option**. The `Reboot` dialog box appears with the following message: `Do you want to shutdown and reboot the computer?`

STEP 2: **Reboot the system**. Click on the `OK` button to reboot the machine. When the reboot is complete, the DII COE Login window appears.

6.2.3 Disk Manager Option

The `Disk Manager` option provides the following file system management functionality:

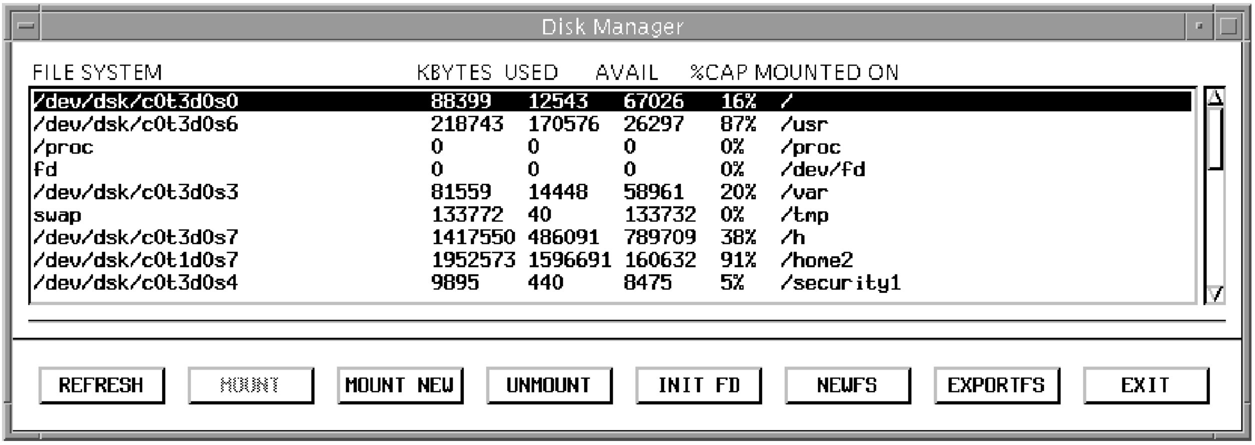
C Mounts file system partitions

C Formats hard drives

C Displays hard disk space availability

C Initializes floppy diskettes.

After selecting the `Disk Manager` option, the `Disk Manager` window appears (Figure 8).



```
FILE SYSTEM                       KBYTES  USED    AVAIL   %CAP MOUNTED ON
/dev/dsk/c0t3d0s0                 88399   12543   67026   16%  /
/dev/dsk/c0t3d0s6                 218743  170576  26297   87%  /usr
/proc                             0       0       0       0%   /proc
fd                                0       0       0       0%   /dev/fd
/dev/dsk/c0t3d0s3                 81559   14448   58961   20%  /var
swap                              133772  40      133732  0%   /tmp
/dev/dsk/c0t3d0s7                 1417550 486091  789709  38%  /h
/dev/dsk/c0t1d0s7                 1952573 1596691 160632  91%  /home2
/dev/dsk/c0t3d0s4                 9895    440     8475    5%   /security1
```

Figure 8. Disk Manager Window

A mounted file system can be accessed for read and write operations. Mounted file systems are highlighted in yellow.

Disk Manager Window Buttons

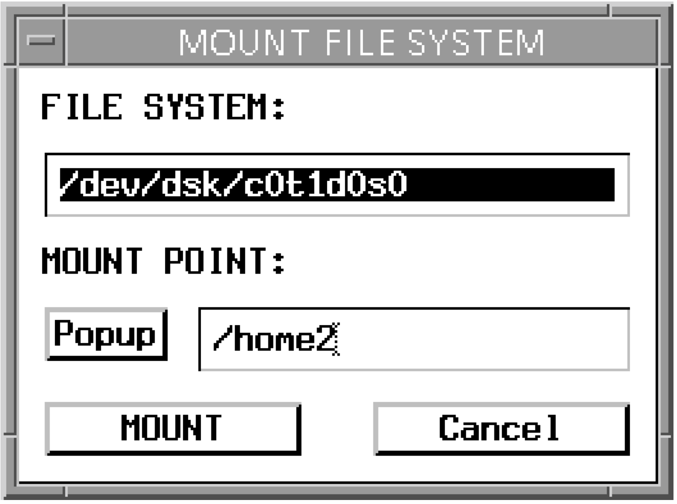
The `Disk Manager` window has the following buttons: `REFRESH`, `MOUNT`, `MOUNT NEW`, `UNMOUNT`, `INIT FD`, `NEWFS`, `EXPORTFS`, and `EXIT`. These buttons are described below.

`REFRESH`
Used to update file system entries in the `Disk Manager` window.

`MOUNT`
Used to attach an existing file system listed in the `Disk Manager` window to a directory, thereby making the files available to the user. Follow the steps below to mount a file system.

STEP 1: **Select a file system to be mounted**. Click on a file system in the `Disk Manager` window to highlight it.

STEP 2: **Click on the `MOUNT` button**. The `MOUNT FILE SYSTEM` window appears (Figure 9).



MOUNT FILE SYSTEM

FILE SYSTEM: /dev/dsk/c0t1d0s0

MOUNT POINT: /home2

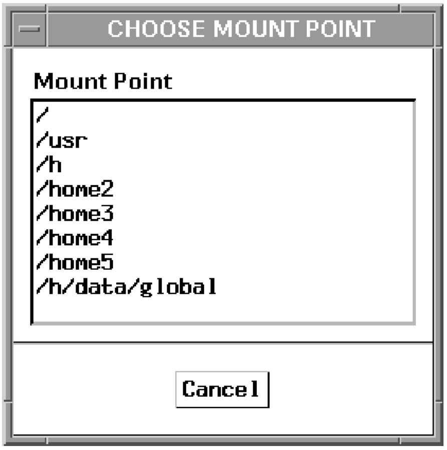
Figure 9. MOUNT FILE SYSTEM Window

STEP 3: **Select an unused location as a mount point for the file system**. Enter a mount point in the `MOUNT POINT` field. Enter a mount point in one of two ways:

(a) Type the location, if known, in the `MOUNT POINT` field.

OR

(b) Toggle on the `Popup` checkbox to the left of the `MOUNT POINT` field to open the `CHOOSE MOUNT POINT` window (Figure 10). Click on a mount point from the scroll list to select it. The `MOUNT FILE SYSTEM` window reappears with the new mount point in the `FILE SYSTEM` field.



CHOOSE MOUNT POINT

Mount Point

```
/
/usr
/h
/home2
/home3
/home4
/home5
/h/data/global
```

Figure 10. CHOOSE MOUNT POINT Window

STEP 4: **Mount the file system**. Click on the MOUNT button in the MOUNT FILE SYSTEM window.

STEP 5: **Determine if the file system should be mounted each time the system is rebooted**. Select YES or NO at the following prompt: Do you want to permanently mount the file system?If you select NO, then that data will not be available to the user the next time the machine is rebooted.

MOUNT NEW

Used to identify a new file system and attach it to a directory, thereby making that directory structure available to the user. Once mounted, the file system is listed in the Disk Manager window. Follow the steps below to identify a new file system:

STEP 1: **Click on the MOUNT NEW button**. The MOUNT FILE SYSTEM window appears (Figure 9).

STEP 2: **Select the new file system to be created**. Enter the new file system name in the FILE SYSTEM field.

STEP 3: **Select an unused location as a mount point for the file system**. Enter a mount point in the MOUNT POINT field to select an unused location to mount the file system. Enter a mount point in one of two ways:

(a) Type the location, if known, in the MOUNT POINT field.

OR

(b) Toggle on the Popup checkbox to the left of the MOUNT POINT field to open the CHOOSE MOUNT POINT window (Figure 10).Click on a mount point from the scroll list to select it. The MOUNT FILE SYSTEM window reappears with the new mount point in the FILE SYSTEM field.

STEP 4: **Mount the new file system**. Click on the MOUNT button in the MOUNT FILE SYSTEM window.

STEP 5: **Determine if the file system should be mounted each time the system is rebooted**. Select YES or NO at the following prompt: Do you want to permanently mount the file system?If you select NO, then that data will not be available to the user the next time the machine is rebooted.

UNMOUNT

Used to unattach a file system listed in the Disk Manager window to a directory. When a file system is unmounted, the files become unavailable to the user, yet they remain intact.

NOTE: A file system that is in use cannot be unmounted.

Follow the steps below to unmount a file system.

STEP 1: **Select a file system to be unmounted**. Click on a file system in the `Disk Manager` window to highlight it.

STEP 2: **Click on the `UNMOUNT` button**.

STEP 3: **Determine if the file system should be permanently unmounted**. Select `YES` or `NO` at the following prompt: `DO YOU WANT TO PERMANENTLY UNMOUNT THE FILESYSTEM?` If you select `NO`, then that data will be available to the user the next time the machine is rebooted.

`INIT FD`

Used to format a floppy diskette. Follow the steps below to format a floppy diskette.

STEP 1: **Click on the `INIT FD` button**.

STEP 2: **Confirm that the floppy diskette should be formatted**. Click on the `CONTINUE` button in the `WARNING` window to initialize the disk, or click on the `CANCEL` button to return to the `Disk Manager` window.

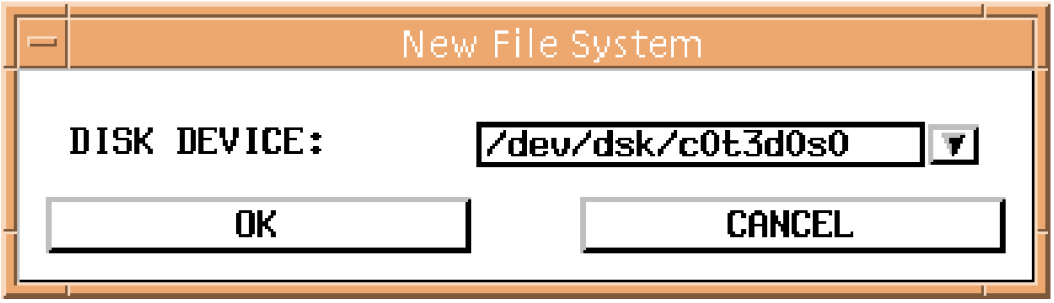
WARNING: The `INIT FD` option erases the entire contents of the floppy diskette.

`NEWFS`

Used to reformat a selected device to create a new file system. Follow the steps below to create a new file system.

WARNING: All data on the selected device will be deleted. No partitions are protected from NEWFS. Therefore, it is advised that you back up any data you want to save before beginning any NEWFS procedure.

STEP 1: **Click on the `NEWFS` button**. The `New File System` window appears (Figure 11).



/dev/dsk/c0t3d0s0

Figure 11. New File System Window

STEP 2: **Select the disk device to be reformatted**. Select the device in one of two ways:

(a) Type the name of the disk device in the `DISK DEVICE` field.

OR

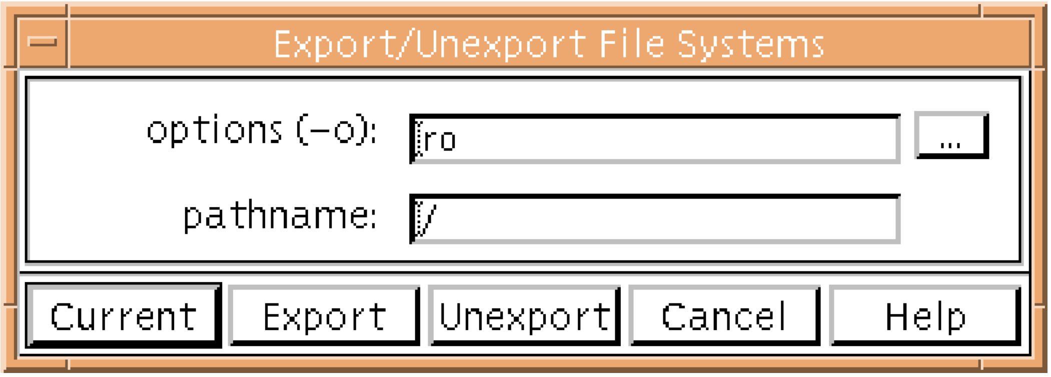
(b) Click on the arrow and then click on a disk device from the list to select it.

STEP 3: **Click on the `OK` button**.

STEP 4: **Confirm that the new file system should be created**. Click on the `CONTINUE` button in the `WARNING` window to format the device, or click on the `CANCEL` button to discard the process.

EXPORTFS

Used to export or unexport a file system in order to allow or deny file system sharing. After selecting the `EXPORTFS` option, the `Export/Unexport File Systems` window appears (Figure 12).



options (-o): ro

pathname: /

Figure 12. Export/Unexport File Systems Window

Export/Unexport File Systems Window Buttons

`Current`
Used to show the file systems that are currently exported (shared).

`Export`
Used to export (share) a selected file system permanently.

`Unexport`
Used to unexport (deny file system sharing to) a selected file system permanently.

`Cancel`
Used to close the `Export/Unexport File Systems` window.

`Help`
Used to show a manual page for the `EXPORTFS` option.

Follow the steps below to export a file system.

STEP 1: **Select a file system**. Click on a file system in the list in the `Disk Manager` window to highlight it and then click on the `EXPORTFS` button. The `Export/Unexport File Systems` window appears (Figure 12).

STEP 2: **Enter options**. Click on the `options` field toggle to view a list of options. Click on one or more options from the list (e.g., read only, read/write) to select them. The options then appear in the `options` field.

STEP 3: **Enter a pathname**. Enter the actual pathname of the directory you want to share in the `pathname` field.

STEP 4: **Export the file system**. Click on the `Export` button.

STEP 5: **Determine if the file system should be exported or unexported permanently**. Click on the `Yes` or the `No` button when the following prompt appears: `Do you want to permanently export the file system?` The window closes.

STEP 6: **Confirm that the file was exported**. Click on the `Current` button in the `Disk Manager` window. The shared directory should appear in the list of exported file systems.

NOTE: Refer to the EXPORTFS manual page for more information about the `EXPORTS` option. Click on the `Help` button in the `Export/Unexport File Systems` window to view the EXPORTFS manual page.

EXIT

Used to close the `Disk Manager` window and exit the `Disk Manager` option.

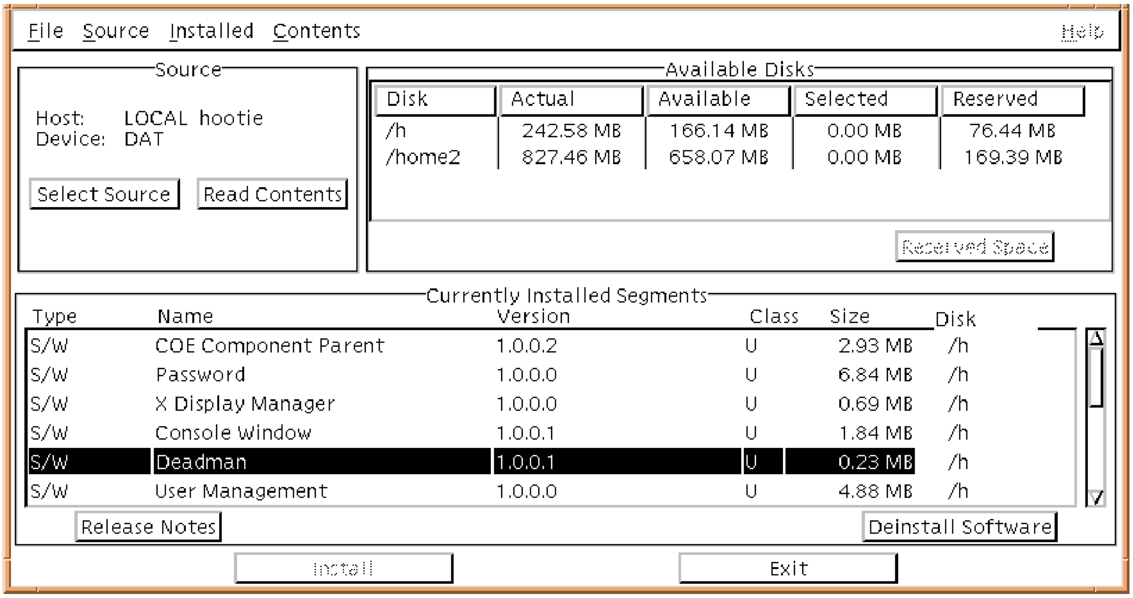
6.3 Software Menu

The `Software` menu contains two options: `Segment Installer` and `Segment Installation Server`. These options are described in the following subsections.

6.3.1 Segment Installer Option

The `Segment Installer` option is used to install segments. Select the `Segment Installer` option to open the `Installer` window (Figure 13).

> **NOTE**: Ensure that you can see the whole window by clicking on the bottom right edge of the window and dragging the trackball or mouse outward to enlarge the window.



Host: LOCAL hootie
Device: DAT

Disk	Actual	Available	Selected	Reserved
/h	242.58 MB	166.14 MB	0.00 MB	76.44 MB
/home2	827.46 MB	658.07 MB	0.00 MB	169.39 MB

Type	Name	Version	Class	Size	Disk
S/W	COE Component Parent	1.0.0.2	U	2.93 MB	/h
S/W	Password	1.0.0.0	U	6.84 MB	/h
S/W	X Display Manager	1.0.0.0	U	0.69 MB	/h
S/W	Console Window	1.0.0.1	U	1.84 MB	/h
S/W	Deadman	1.0.0.1	U	0.23 MB	/h
S/W	User Management	1.0.0.0	U	4.88 MB	/h

Figure 13. Installer Window

6.3.1.1 Installer Window Pull-down Menus

The `Installer` window has the following pull-down menus: `File`, `Source`, `Installed`, and `Contents`. These pull-down menus are described below.

File

The `File` pull-down menu contains the following options: `Install` and `Exit`.

Install
Allows the user to install selected segments. Performs the same functionality as clicking on the `Install` button. Refer to Subsection 6.3.1.2, *Installer Window Panels,* for more information about the `Install` button.

Exit
Exits the user from the `Installer` window. Performs the same functionality as clicking on the `Exit` button. Refer to Subsection 6.3.1.2, *Installer Window Panels,* for more information about the `Exit` button.

Source

The `Source` pull-down menu contains the following options: `Select Source` and `Read Contents`.

Select Source
Displays the currently selected installation media. Performs the same functionality as clicking on the `Select Source` button. Refer to Subsection 6.3.1.2, *Installer Window Panels,* for more information about the `Select Source` button.

Read Contents
Allows the user to read the table of contents of the selected installation device. Performs the same functionality as clicking on the `Read Contents` button. Refer to Subsection 6.3.1.2, *Installer Window Panels,* for more information about the `Read Contents` button.

Installed

The `Installed` pull-down menu contains the following options: `Release Notes`, `Deinstall Software`, and `View Installation Log`.

Release Notes
Displays release notes information for any selected segment. Performs the same functionality as clicking on the `Release Notes` button. Refer to Subsection 6.3.1.2, *Installer Window Panels,* for more information about the `Release Notes` button.

Deinstall Software
Allows the user to deinstall segments highlighted in the `Currently Installed Segments` panel. Performs the same functionality as clicking on the `Deinstall Software` button. Refer to Subsection 6.3.1.2, *Installer Window Panels*, for more information about the `Deinstall Software` button.

View Installation Log
Displays a detailed log of the installation process.

Contents

The `Contents` pull-down menu contains the following options: `Release Notes`, `Required Software`, and `Conflicting Software`.

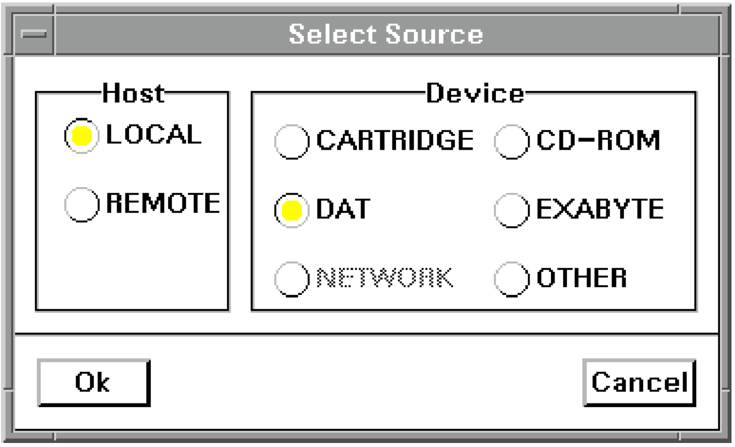
> **Release Notes**
> Displays release notes information for any selected segment. Performs the same functionality as clicking on the `Release Notes` button. Refer to Subsection 6.3.1.2, *Installer Window Panels*, for more information about the `Release Notes` button.
>
> **Required Software**
> Lists segments that need to be installed in order to install the segment selected in the `Select Segment To Install` panel. Performs the same functionality as clicking on the `Requires` button. Refer to Subsection 6.3.1.2, *Installer Window Panels*, for more information about the `Requires` button.
>
> **Conflicting Software**
> Lists the segments that cannot be installed with the segment selected in the `Select Segment To Install` panel. Performs the same functionality as clicking on the `Conflicts` button. Refer to Subsection 6.3.1.2, *Installer Window Panels*, for more information about the `Conflicts` button.

6.3.1.2 Installer Window Panels

The `Installer` window has the following panels: `Source`, `Available Disks`, `Currently Installed Segments`, and `Select Software To Install`. The `Select Software To Install` panel does not appear in the `Installer` window shown in Figure 13—it only appears after the `Read Contents` button has been selected in the `Source` panel. The `Installer` window panels are described below.

Source
Displays the name of the host machine, the name of the installation device, and the table of contents of that installation device. The `Source` panel has two buttons: `Select Source` and `Read Contents`.

> **Select Source**
> Used to display the currently selected installation media. Click on the `Select Source` button to open the `Select Source` window (Figure 14). This window allows the user to select the installation source device. The device selection defaults to the DAT drive on the local machine (the `LOCAL` option in the `Host` panel and the `DAT` option in the `Device` panel).



Select Source

Host

● LOCAL

○ REMOTE

Device

○ CARTRIDGE ○ CD-ROM

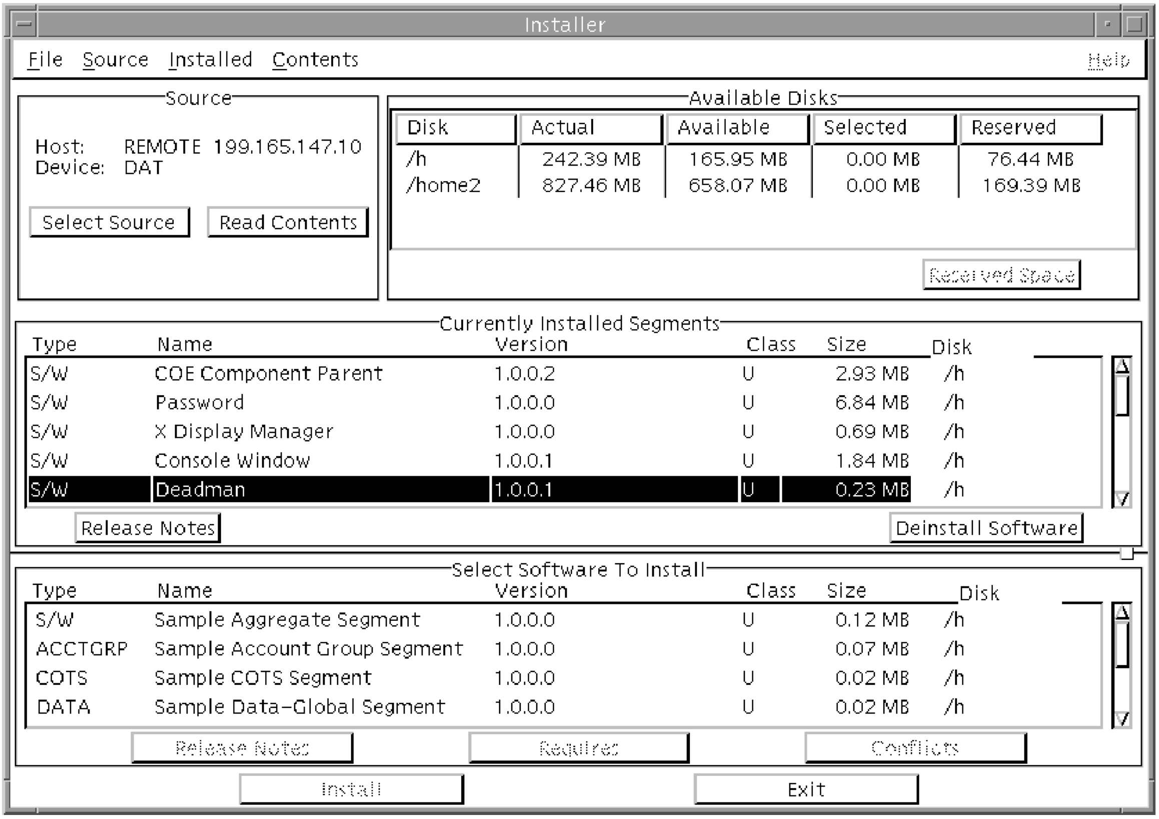
● DAT ○ EXABYTE

○ NETWORK ○ OTHER

Figure 14. Select Source Window

`Read Contents`

Used to read the table of contents of the selected installation device. Click on a segment listed in the `Installer` window to highlight it and then click the `Read Contents` button. The media will be scanned for the segments that it contains, and then the `Installer` window will add the `Select Software To Install`panel, which lists the segments that the media contains (Figure 15). Any number of segments may be selected in this panel for installation. See Section 6.3.1.3, *Installing Segments*, for additional information about the segment installation process.



Host: REMOTE 199.165.147.10
Device: DAT

Disk	Actual	Available	Selected	Reserved
/h	242.39 MB	165.95 MB	0.00 MB	76.44 MB
/home2	827.46 MB	658.07 MB	0.00 MB	169.39 MB

Type	Name	Version	Class	Size	Disk
S/W	COE Component Parent	1.0.0.2	U	2.93 MB	/h
S/W	Password	1.0.0.0	U	6.84 MB	/h
S/W	X Display Manager	1.0.0.0	U	0.69 MB	/h
S/W	Console Window	1.0.0.1	U	1.84 MB	/h
S/W	Deadman	1.0.0.1	U	0.23 MB	/h

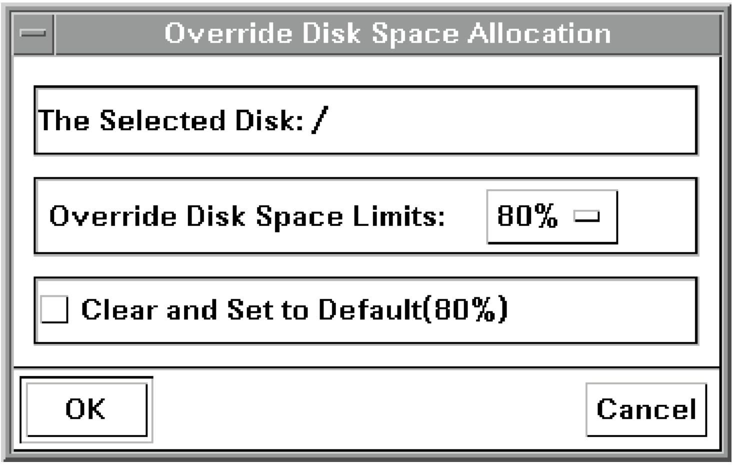
Type	Name	Version	Class	Size	Disk
S/W	Sample Aggregate Segment	1.0.0.0	U	0.12 MB	/h
ACCTGRP	Sample Account Group Segment	1.0.0.0	U	0.07 MB	/h
COTS	Sample COTS Segment	1.0.0.0	U	0.02 MB	/h
DATA	Sample Data-Global Segment	1.0.0.0	U	0.02 MB	/h

Figure 15. Installer Window with Select Software To Install Panel

`Available Disks`
Displays the mounted disk drives on the system and the remaining available disk space. The amount of available disk space decreases as segments are selected for installation. This panel has five fields: `Disk`, `Actual`, `Available`, `Selected`, and `Reserved`.

> **`Disk`**
> Shows each available disk.
>
> **`Actual`**
> Shows the total size of each disk.
>
> **`Available`**
> Shows the free space that is available on each disk for installing segments.
>
> **`Selected`**
> Shows the size of the segment(s) you want to add or remove based on your selection of one or more segments in the `Currently Installed Segments`panel.
>
> **`Reserved`**
> Shows the amount of space on each disk that is already in use or pre-allocated (reserved) by previously installed segments.

The `Available Disks` panel has the following button: `Reserved Space`. The system automatically reserves a certain amount of space on each available disk to allow for segment growth. The `Reserved Space` button allows the reserved disk space to be modified for a particular installation. To modify reserved disk space for a particular installation, click on a disk in the list to highlight it and then click on the `Reserved Space` button to open the `Override Disk Space Allocation` window (Figure 16). The `Override Disk Space Limits` pop-up menu allows the user to choose between 80 percent and 100 percent of space to install the segment.



The Selected Disk: /

Override Disk Space Limits: 80%

□ Clear and Set to Default(80%)

Figure 16. Override Disk Space Allocation Window

Currently Installed Segments

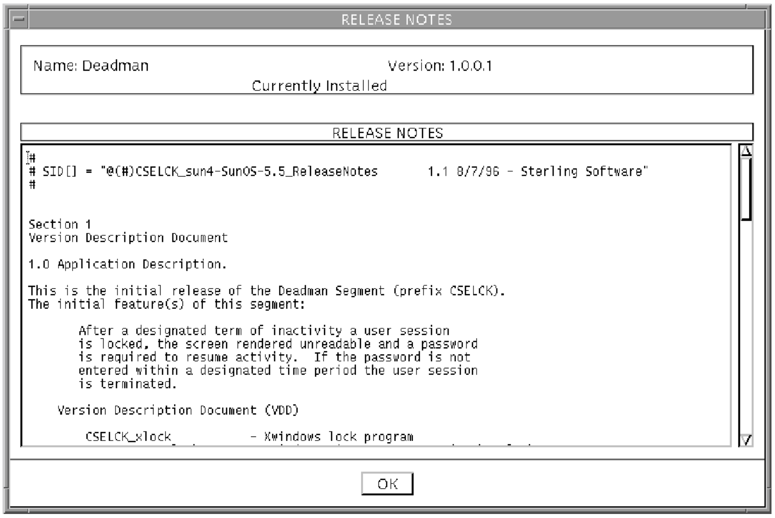
Lists the segments that are currently installed. The `Currently Installed Segments` panel lists the type, name, version number, classification, size, and disk (mount point) of each currently installed segment. This panel has two buttons: `Release Notes` and `Deinstall Software`.

Release Notes

Displays release notes information for any selected segment. Click on a segment to highlight it and click on the `Release Notes` button to open the `RELEASE NOTES` window (Figure 17).

Deinstall Software

Allows the user to deinstall segments highlighted in the `Currently Installed Segments` panel.



Name: Deadman   Version: 1.0.0.1

Currently Installed

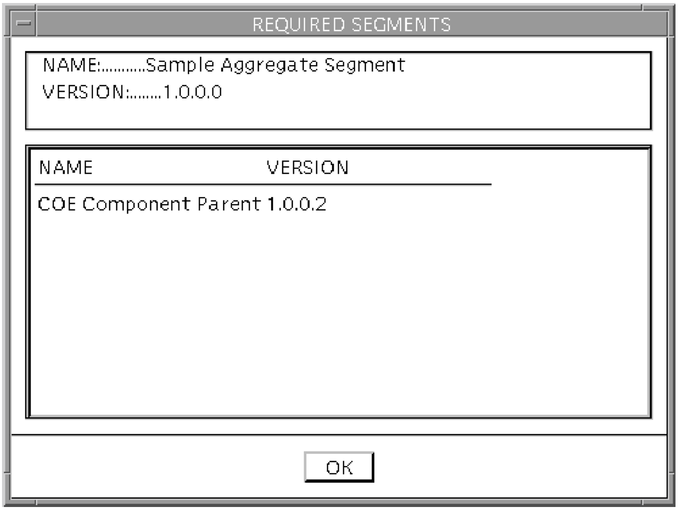
```
#
# SID[] = "@(#)CSELCK_sun4-SunOS-5.5_ReleaseNotes      1.1 8/7/96 - Sterling Software"
#


Section 1
Version Description Document

1.0 Application Description.

This is the initial release of the Deadman Segment (prefix CSELCK).
The initial feature(s) of this segment:

       After a designated term of inactivity a user session
       is locked, the screen rendered unreadable and a password
       is required to resume activity.  If the password is not
       entered within a designated time period the user session
       is terminated.

    Version Description Document (VDD)

        CSELCK_xlock           - Xwindows lock program
```

Figure 17. RELEASE NOTES Window

`Select Software To Install`

Lists the segments that are contained on the selected media and that are not currently installed. The `Select Software To Install`panel lists the type, name, version number, classification, size, and mount point (disk) of each segment contained on the media. This panel has five buttons: `Release Notes`, `Requires`, `Conflicts`, `Install`, and `Exit`.

> **`Release Notes`**
>
> Displays release notes information for any selected segment. Click on a segment to highlight it and click on the `Release Notes` button to open the `RELEASE NOTES` window (Figure 17).
>
> **`Requires`**
>
> Lists segments that need to be installed in order to install the segment selected in the `Select Segment To Install`panel. Click on a segment to highlight it and click on the `Requires` button to open the `REQUIRED SEGMENTS` window (Figure 18).

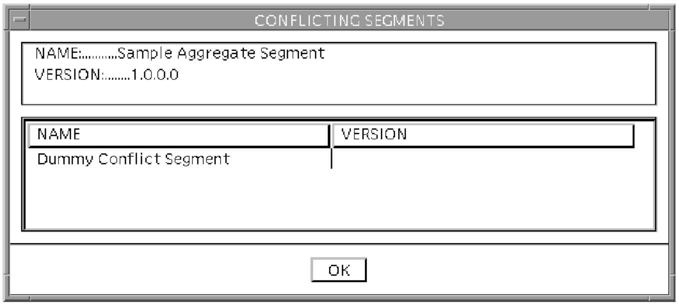


NAME:...........Sample Aggregate Segment
VERSION:........1.0.0.0

NAME	VERSION
COE Component Parent 1.0.0.2	

Figure 18. REQUIRED SEGMENTS Window

`Conflicts`
Lists the segments that cannot be installed with the segment selected in the `Select Segment To Install` panel. Click on a segment to highlight it and click on the `Conflicts` button to open the `CONFLICTING SEGMENTS` window (Figure 19).



NAME:..........Sample Aggregate Segment
VERSION:........1.0.0.0

NAME	VERSION
Dummy Conflict Segment	

Figure 19. CONFLICTING SEGMENTS Window

`Install`
Allows the user to install selected segments.

`Exit`
Exits the user from the `Installer` window.

6.3.1.3 Installing Segments

Follow the steps below to install segments using the `Segment Installer` option.

STEP 1: **Select the installation device**. Click on the `Select Source` button in the `Source` panel to open the `Select Source` window (Figure 14). Select the device to use as the installation source device. Select `NETWORK` if you are installing a segment from the segment installation server. Refer to Section 6.3.2, *Segment Installation Server Option*, for information about loading segments on the segment installation server.

STEP 2: **Read the table of contents of the selected installation device**. Click on the `Read Contents` button in the `Source` panel. The media will be scanned for the segments that it contains, and then the `Installer` window will add the `Select Software To Install` panel, which lists the segments that the media contains (Figure 15). Any number of segments may be selected in this panel for installation.

STEP 3: **Select the segments that you want to install**. Click on one or more segments in the `Select Software To Install` panel. The `Available Disks` panel then displays the mounted disk drives on the system and the remaining available disk space as segments are selected.

STEP 4: **Begin the installation process for the selected segments**. Click on the `Install` button once all desired segments are selected. The `Installer Status` window appears, which shows the number of segments to be installed and the size of each segment being installed. This window also shows a `Percent Complete` status bar, which shows the status of the installation.

STEP 5: **Display a detailed log of the installation process**. Select the `Installation Log` option from the `Installed` pull-down menu once installation has completed.

6.3.2 Segment Installation Server Option

The `Segment Installation Server` option is used to load segments onto a segment server. Loading a segment is different than installing a segment. Loading a segment on a machine stores the segment on the machine, but does not enable the segment to run. Instead, segments stored on a segment installation server are available for installation without the installation media because they are located on a server. Segments can, then, be installed individually on each machine on the network.

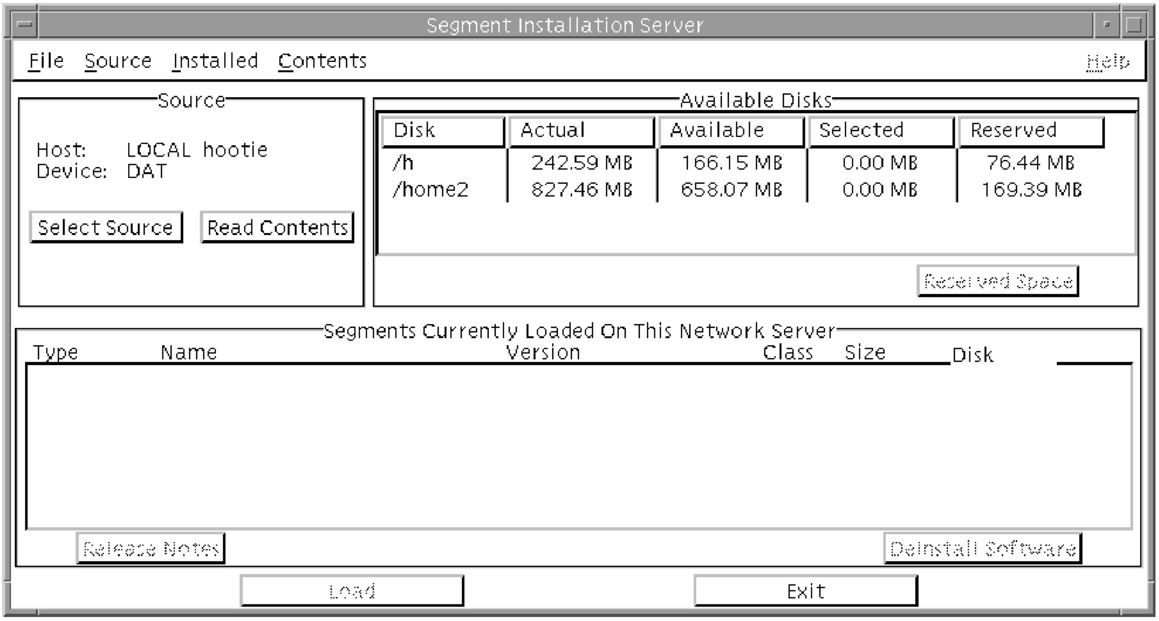
Click on the `Segment Installation Server` option to open the `Segment Installation Server` window (Figure 20). This window is identical to the `Installer` window, with the following exceptions:

C The `Load` option in the `File` pull-down menu replaces the `Install` option.

C The `Load` button replaces the `Install` button.

C The `Segments Currently Loaded On This Network Server`panel replaces the `Currently Installed Segments`panel.

NOTE: Ensure that you can see the whole window by clicking on the bottom right edge of the window and dragging the trackball or mouse outward to enlarge the window.



Host: LOCAL hootie
Device: DAT

Disk	Actual	Available	Selected	Reserved
/h	242.59 MB	166.15 MB	0.00 MB	76.44 MB
/home2	827.46 MB	658.07 MB	0.00 MB	169.39 MB

Type	Name	Version	Class	Size	Disk

Figure 20. Segment Installation Server Window

6.3.2.1 Loading Segments on the Segment Installation Server

NOTE: The following must be done for the network installation to be successful:

C The `/h/data/global` directory must be mounted to a common machine. If `/h/data/global` is not mounted, use the `Disk Manager` option from the `Hardware` pull-down menu to mount it (see Subsection 6.2.3, *Disk Manager Option*).

C Segments installed from a segment installation server must have been loaded on `/home2` or on any other exported file system on the server machine; if they are not, the COEInstaller will not be able to access the segments. The machine that the segments are being installed from must be in the target machine's host file or, if running DNS, then the host must be in the DNS file.

Follow the steps below to load a segment on the segment installation server.

STEP 1: **Select a server on which to load segments**. Select a disk in the `Available Disks` panel. A list of segments, which can be installed from the `Installer` window, is created automatically in the `/h/data/global` directory and is updated each time a segment is loaded using this option.

STEP 2: **Select the installation device**. Click on the `Select Source` button in the `Source` panel to open the `Select Source` window (Figure 14). Select the installation source device and then click on the `OK` button.

STEP 3: **Select the segments that you want to load**. Click on one or more segments in the `Select Software To Install` panel. The `Available Disks` panel then displays the mounted disk drives on the system and the remaining available disk space as segments are selected.

STEP 4: **Begin the load process for the selected segments**. Click on the `Load` button once all desired segments are selected. The `Installer Status` window appears, which shows the number of segments to be loaded and the size of each segment being loaded. This window also shows a `Percent Complete` status bar, which shows the status of the load.

STEP 5: **Display a detailed log of the load process**. Select the `Installation Log` option from the `Installed` pull-down menu once the load has completed.

Follow the steps in Section 6.3.1.3, *Installing Segments*, to install one or more segments on a machine.

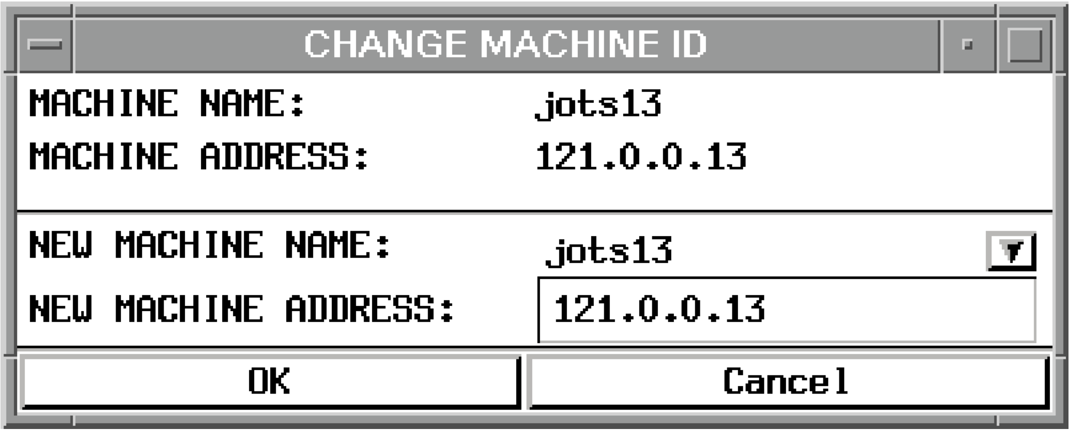
6.4 Network Menu

The `Network` menu contains the following options: `Change Machine ID`, `Edit Local Hosts`, `Set System Time`, `Servers`, and `DCE`. These options are described in the following subsections.

6.4.1 Change Machine ID Option

Use the `Change Machine ID` option to select a name and IP address for a machine. Click on this option to open the `CHANGE MACHINE ID` window (Figure 21). The machine's current name and IP address appear in the `MACHINE NAME` and `MACHINE ADDRESS` fields.

> **NOTE**: A machine's name (ID) and IP address are selected initially during system installation.
>
> **NOTE**: All machines must have unique names and addresses—the system does not permit two machines to have the same name and address.



MACHINE NAME: jots13
MACHINE ADDRESS: 121.0.0.13
NEW MACHINE NAME: jots13
NEW MACHINE ADDRESS: 121.0.0.13

Figure 21. CHANGE MACHINE ID Window

Follow the steps below to change the machine ID.

STEP 1: **Select a new machine**. Click on the arrow to the right of the `NEW MACHINE NAME` field to display a pop-up list of valid IDs.

STEP 2: **Select an ID.** Click on an ID to select it.

> **NOTE**: User-defined names may be assigned to each machine using the `Edit Local Hosts` option before changing the machine ID (see Subsection 6.4.2, *Edit Local Hosts Option*).

STEP 3: **Click on the `OK` button**. The `MACHINE NAME` and `MACHINE ADDRESS` fields update to reflect the new machine name and address.

STEP 4: **Reboot the machine**. Reboot the machine after changing the name for the change to take effect.

> **NOTE**: Do not modify the `NEW MACHINE ADDRESS` field. Machine addresses are predefined for each ID.

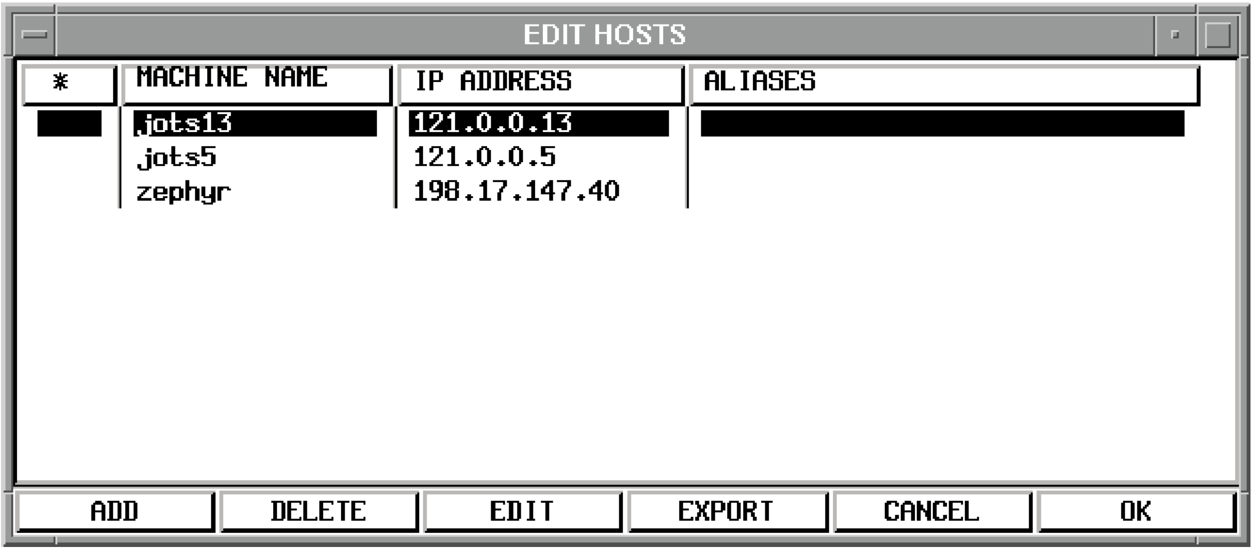
6.4.2 Edit Local Hosts Option

The `Edit Local Hosts` option lists the machines that can be accessed from a user's machine. This option can only be used on local workstation files. Use this option to do the following:

C Add or remove machines from the list of machines that can be accessed

C Modify machine information, such as machine name, IP address, or aliases.

Select the `Edit Local Hosts` option to open the `EDIT HOSTS` window (Figure 22).



*	MACHINE NAME	IP ADDRESS	ALIASES
	jots13	121.0.0.13	
	jots5	121.0.0.5	
	zephyr	198.17.147.40	

Figure 22. EDIT HOSTS Window

Follow the steps below to modify machine information. These steps must be performed for each machine you want to modify.

STEP 1: **Modify host file information**. Use the `Edit Local Hosts` option to add or remove machines from the list or to modify machine information. Once you have completed the selected action, the machine remains in the `EDIT HOSTS` window labeled with `A` (add), `M` (modify), or `D` (delete) in the `*` column. Click on the `OK` button to accept the changes, or click on the `CANCEL` button to discard the changes.

STEP 2: **Assign the machine a new machine name**. Assign the machine a new machine name using the `Change Machine ID` option (see Subsection 6.4.1, *Change Machine ID Option*).

STEP 3: **Reboot the machine**. Reboot the machine at the prompt if you modified the current hostname in order for changes to take effect.

6.4.2.1 EDIT HOSTS Window Fields

The `EDIT HOSTS` window has the following fields: * (asterisk), `MACHINE NAME`, `IP ADDRESS`, and `ALIASES`. These fields are described below.

*** (asterisk)**
Shows pending changes made to the machine. Labels include `A` (add), `D` (delete), `M` (modify), and `T` (trusted).

The label T indicates a trusted machine. A trusted machine can be accessed from another machine on the same LAN (e.g., to access a tape drive for remote installation). A trusted machine is one that can access the user's disk and perform remote shell commands.

MACHINE NAME
Shows the name of the machine. The machine name can be system or user defined.

IP ADDRESS
Shows a unique IP address.

ALIASES
Shows other names by which a machine is also known, if applicable.

6.4.2.2 EDIT HOSTS Window Buttons

The EDIT HOSTS window has the following buttons: ADD, DELETE, EDIT, EXPORT, CANCEL, and OK. These buttons are described below.

ADD
Used to add a machine to the local host table to make it available to the local machine. Follow the steps below to add a machine to the local host table.

STEP 1: **Click on the ADD button**. The ADD MACHINE window appears (Figure 23).

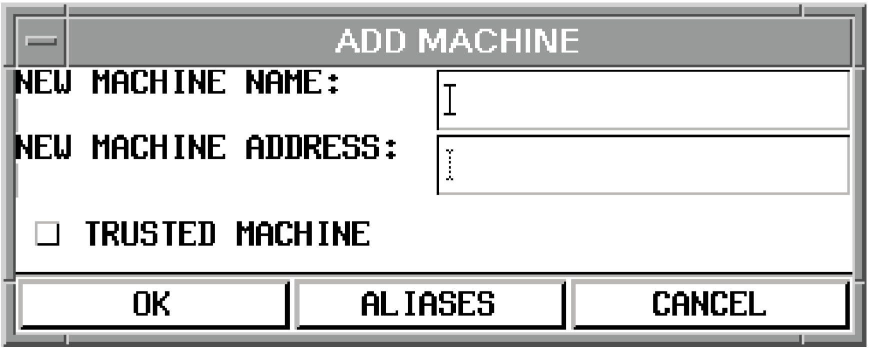


Figure 23. ADD MACHINE Window

STEP 2: **Enter the new machine name**. Type a name in the NEW MACHINE NAME field. Allowable characters are alphanumeric and the underscore symbol (_). In addition, the first character of the machine name must be a letter.

STEP 3: **Enter the machine’s IP address**. Type the IP address of the new machine in the NEW MACHINE ADDRESS field.

STEP 4: **Define the new machine as a trusted machine**. Click on the TRUSTED MACHINE checkbox toggle.

STEP 5: **Add aliases for a machine, if desired**. Click on the ALIASES button in the ADD MACHINE window to open the ALIASES window (Figure 24).

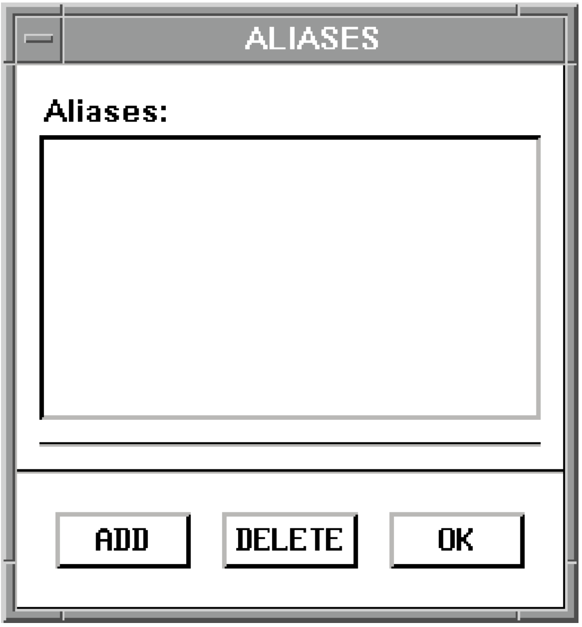


Figure 24. ALIASES Window

To add an alias, click on the ADD button. The ADD ALIAS window appears (Figure 25). Type a new alias in the NEW ALIAS field and then press [RETURN] to accept the new alias. Allowable characters are alphanumeric and the underscore symbol (_). In addition, the first character of the machine name must be a letter. The ALIASES window reappears.

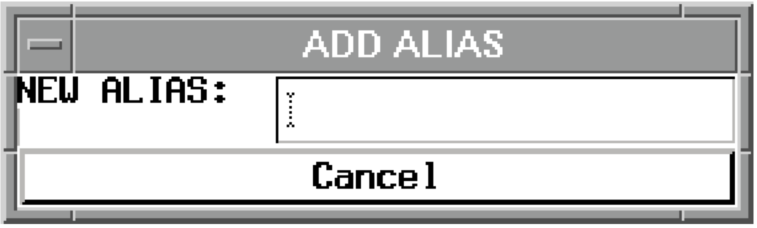


Figure 25. ADD ALIAS Window

STEP 6: **Close the ALIASES window and save the changes**. Click on the OK button. The ADD MACHINE window returns to the forefront.

STEP 7: **Determine if the machine should be added to the list of available machines**. Click on the OK button to mark the machine as an addition to the list of available machines on the local host table, or click on the CANCEL button to discard the changes. The ADD MACHINE window closes.

DELETE

Used to delete a machine from the local host table. Follow the steps below to delete a machine from the local host table.

STEP 1: **Select a machine**. Click on a machine in the list to highlight it.

STEP 2: **Click on the `DELETE` button**. The `DELETE MACHINE` dialog box appears with the following prompt: `Mark machine [machine name] for deletion?`

STEP 3: **Confirm whether or not the machine should be deleted**. Click on the `YES` button to confirm that the machine should be deleted, or click on the `NO` button to cancel the deletion.

EDIT

Used to edit a machine name. Click on a machine name to highlight it and click on the `EDIT` button to open the `EDIT MACHINE` window (Figure 26). The `EDIT MACHINE` window functions the same as the `ADD MACHINE` window (described in **ADD**).

EXPORT

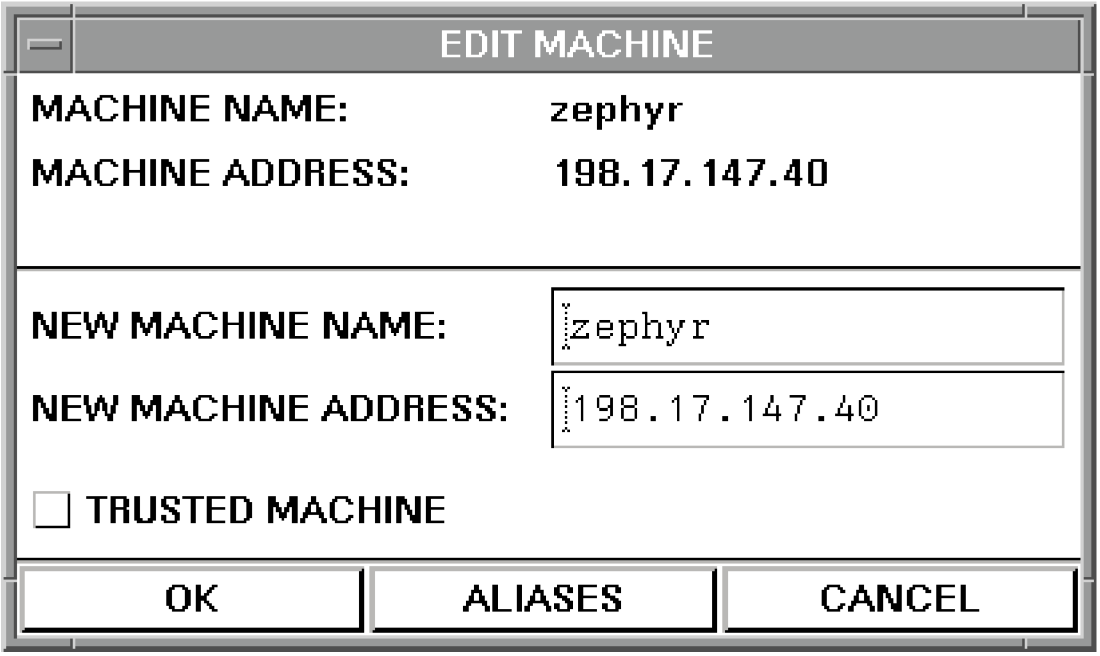
Used to export machine information to other workstations on the local host table. (Not currently implemented.)

CANCEL

Used to close the `EDIT HOSTS` window without saving changes.

OK

Used to save changes and close the window.



MACHINE NAME: zephyr

MACHINE ADDRESS: 198.17.147.40

NEW MACHINE NAME: zephyr

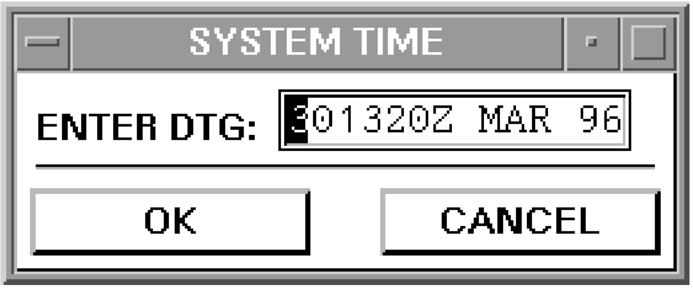
NEW MACHINE ADDRESS: 198.17.147.40

□ TRUSTED MACHINE

Figure 26. EDIT MACHINE Window

6.4.3 Set System Time Option

The `Set System Time` option is used to set the system time for the machine. Click on the `Set System Time` option to open the `SYSTEM TIME` window (Figure 27).



ENTER DTG: 301320Z MAR 96

Figure 27. SYSTEM TIME Window

The system time is written as ddhhmmZ MON YR, where

dd	=	day of the month
hh	=	hour
mm	=	minute
Z	=	a constant (for Zulu time)
MON	=	three-letter month abbreviation
YR	=	final two digits of the year.

For example, October 15, 1996, 8:19 Zulu time would read: 150819Z OCT 96.

To set the system time, follow the steps below:

STEP 1: **Enter the new system time**. Enter the new system time in the `ENTER DTG` field in the format ddhhmmZ MON YR.

STEP 2: **Set the new system time for the machine**. Click on the `OK` button to accept the new entry, or click on the `CANCEL` button to discard the entry.

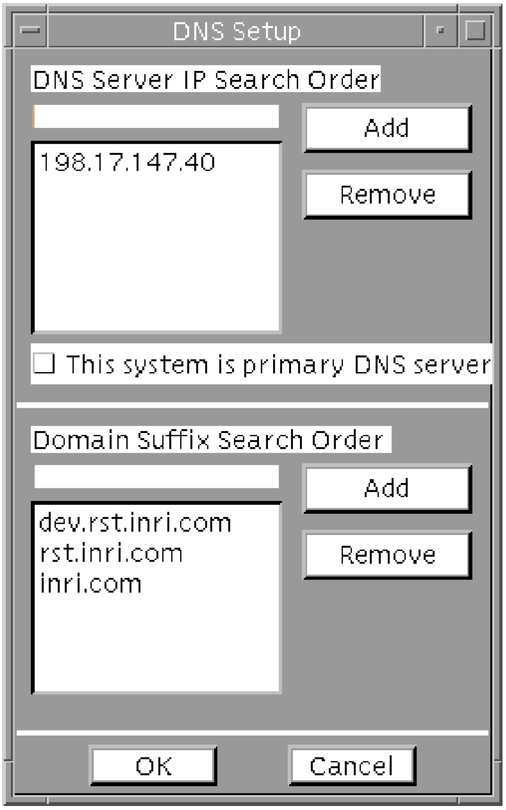
6.4.4 Servers Option

The `Servers` option is a cascading menu that has four options: `Set DNS`, `Set Routes`, `Set Mail`, and `Set NIS`. These options are described in the following subsections.

NOTE: The `Set Mail` option is not available on HP workstations.

6.4.4.1 Set DNS Option

The `Set DNS` option allows the system administrator to configure a workstation as either a Domain Name Server (DNS) client or a DNS server if DNS, rather than the local host table, is used to store host name IP address information. Figure 28 shows the `DNS Setup` window. The `Set DNS` option creates the nameserver configuration file and, upon a positive response, installs a set of DNS template files to `/var/nameserver`. This option allows the system administrator to enter the IP address of the primary and secondary machines. It also allows the system administrator to input suffixes of machine names instead of IP addresses.



DNS Server IP Search Order

198.17.147.40

□ This system is primary DNS server

Domain Suffix Search Order

dev.rst.inri.com
rst.inri.com
inri.com

Figure 28. DNS Setup Window

NOTE: The system administrator must edit the DNS template files manually for proper server configuration.

NOTE: On Solaris 2.x Operating Systems, a new `/etc/nsswitch.conf` file with the appropriate reference to DNS will be installed. The only change to this file is that the DNS references are added. On HP Operating Systems, a new `/etc/resolv.conf` file will be installed that includes the DNS name server list and the domain search list.

If your workstation is acting as the primary DNS server, click on the `Add` button to enter the IP address of the DNS server in the `DNS Server IP Search Order` field and click on the `This system is primary DNS server` toggle. You can also click on the `Add` button to enter the IP address of a backup DNS server in the `DNS Server IP Search Order` field. In addition, you can click on the `Add` button to add multiple domain suffixes in the `Domain Suffix Search Order` field. A domain suffix is a list of suffixes appended to a system name that are used to help locate the system. Click on the `OK` button when finished.

If your workstation is not acting as the primary DNS server, click on the `Add` button to enter the IP address of the primary DNS server in the `DNS Server IP Search Order` field and then enter the IP address of the backup DNS server. Do NOT click on the `This system is primary`

DNS server toggle. You can also click on the Add button to add multiple domain suffixes in the Domain Suffix Search Order field. Click on the OK button when finished.

6.4.4.2 Set Routes Option

The Set Routes option allows the system administrator to configure a workstation with the appropriate routing configuration. Select this option to open the Default Router Setup window (Figure 29). If your workstation is acting as the default router, enter the IP address of the default router in the Default Router IP Address field and click on the This system is default router toggle. If your workstation is not acting as the default router, enter the IP address of the default router in the Default Router IP Address field. Do NOT click on the This system is default router toggle. Click on the OK button when finished.

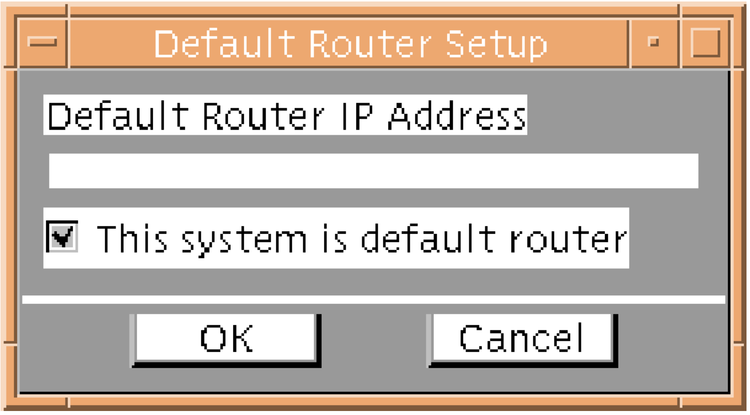


Figure 29. Default Router Setup Window

NOTE: The default router only needs to be configured for access to networks other than the LAN. The default router may also be configured during kernel installation.

6.4.4.3 Set Mail Option

The Set Mail option allows the system administrator to configure mail on a workstation as either a client or a server. Select the Set Mail option to open the Mail Setup window (Figure 30). This option creates the /etc/lib/sendmail.cf file, which is a configuration file used for sending mail. Clicking on the OK button adds an entry into the operating system-specific mount configuration table.

If your workstation is acting as the mail server, enter the mail server IP address in the Default Router IP Address field and click on the This system is mail server toggle. If your workstation is not acting as the mail server, enter the mail server IP address in the Default Router IP Address field. Do NOT click on the This system is mail server toggle. Click on the OK button when finished.

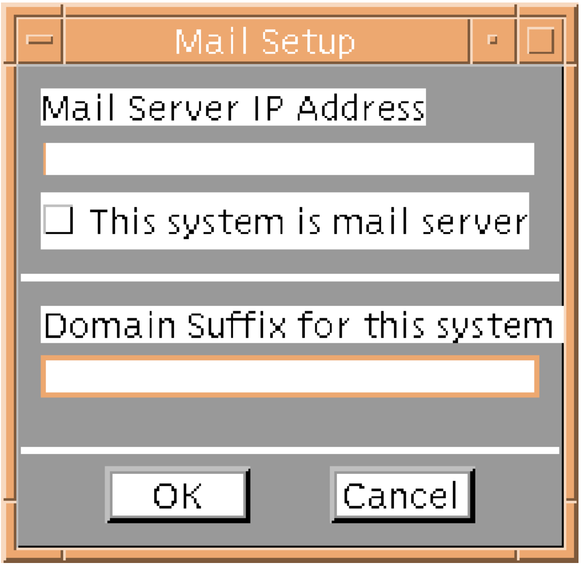


Figure 30. Mail Setup Window

NOTE: The `Set Mail` option is not available on HP workstations.

6.4.4.4 Set NIS Option

Network Information Service (NIS) allows user accounts to be shared across all workstations on the same domain. The `Set NIS` option is used to initialize a machine as a NIS server, add clients, and remove NIS from a machine. The `Set NIS` option is a cascading menu that has three options: `Initialize NIS`, `Add NIS Client`, and `Remove NIS`.

Before NIS can be initialized, DNS must be configured on the master server and on the client machine. Refer to Section 6.4.4.1, *Set DNS Option*, for information on configuring DNS. In addition, an entry must be added to export the global users directory before NIS can be initialized. In other words, one workstation must have `/h/USERS/global` exported (shared) as read/write and must have `anon=0` to allow root access. If `/h/USERS/global` is not mounted, use the `Disk Manager` option from the `Hardware` pull-down menu to mount it, as described in the next subsection.

To initialize NIS, you need to know the NIS domain name, the client host name and client IP address, the NIS server host name, and the network password (also known as the Secure-RPC password). Your system administrator should provide you with this information.

Adding an Entry To Export the Global Users Directory

Follow the steps below to add an entry to export the global users directory.

STEP 1: **Open the `Disk Manager` window**. Select the `Disk Manager` option from the `Hardware` pull-down menu. The `Disk Manager` window appears (Figure 8).

STEP 2: **Select a file system**. Click on a file system in the list to highlight it and then click on the `EXPORTFS` button. The `Export/Unexport File Systems` window appears (Figure 12).

STEP 3: **Enter the appropriate options**. Type `rw,anon=0` in the `options` field to export the global users directory.

STEP 4: **Enter the appropriate pathname**. Type `/h/USERS/global` in the pathname field.

STEP 5: **Export the file system**. Click on the `Export` button.

STEP 6: **Export the file system permanently**. Click on the `Yes` button when the following prompt appears: `Do you want to permanently export the file system?` The window closes.

STEP 7: **Confirm that the file was exported**. Click on the `Current` button in the `Disk Manager` window. The `/h/USERS/global` directory should appear in the list of exported file systems.

NOTE: Refer to Subsection 6.2.3, *Disk Manager Option*, for more information on mounting and exporting file systems.

Initializing NIS on the Master or the Client

Follow the steps below to initialize NIS on the master or the client machine.

NOTE: It is recommended that the master server be initialized before any client machines.

STEP 1: **Initialize NIS**. Select the `Initialize NIS` option from the `Set NIS` cascading menu option.

STEP 2: **Enter the NIS domain name**. An `ENTER A RESPONSE` window appears. Enter the domain name at the prompt and click on the `OK` button or press [`RETURN`]. This is the name of the domain that will include the master and client machines.

STEP 3: **Set the machine as the master server or as a client**. The `RESPOND TO THE QUESTION` window appears with the following prompt: `Is this machine the Master NIS Server?`If the machine is the client, click on the No button and proceed to STEP 4; if the machine is the server, click on the Yes button and proceed to STEP 9.

STEP 4: **Enter the NIS server host name**. The ENTER A RESPONSE window appears with the following prompt: Enter the NIS Server Host Name. Enter the name of the machine designated as the server at the prompt and click on the OK button or press [RETURN].

STEP 5: **Acknowledge that the NIS server host is reachable**. An INFORMATIONAL MESSAGE window appears with the following message: [NIS Server Host Name] is reachable. Click on the OK button or press [RETURN].

STEP 6: **Continue the initialization**. The following message appears:

```
Initializing client [client name] for domain [domain
name] Once initialization is done, you will need to
reboot your machine. Do you want to continue?
```

Type Y and press [RETURN] to continue, or type N and press [RETURN] to exit the script. If you type Y, proceed to STEP 7; if you type N, proceed to STEP 10.

STEP 7: **Enter the network password**. Several messages appear, ending with the following:

```
At the prompt below, type the network password (also
know as the Secure-RPC password) that you obtained
either from your administrator or from running the nis
populate scripts.
Please enter the Secure-RPC password for root:
```

Enter a password described in the NOTE on the next page and press [RETURN].

STEP 8: **Enter the login password for root**. Enter a password at the prompt and press [RETURN]. The following message appears: Your network has been changed to your login one. Your network and login passwords are now the same. Proceed to STEP 10.

NOTE: This password remains in the password file even if NIS is removed from the client machine. The following message will appear if NIS has already been configured and if the password has already been entered.

```
      If the machine was initialized before as a NIS+ client, please enter
the
      root login password as the network password. Or re-type the network
      password that your administrator gave you.
```

Enter the appropriate password and press [`RETURN`]. The following message appears:

```
      Your network has been changed to your login one. Your network and
login
      passwords are now the same.
```

STEP 9: **Enter and confirm a secman password**. The `ENTER A PASSWORD` window appears after several minutes. Enter a secman password and press [`RETURN`]. Re-enter the password to verify it and press [`RETURN`]. Then click on the `OK` button.

STEP 10: **Acknowledge that the machine needs to be rebooted**. An `INFORMATIONAL MESSAGE` window appears with the following message: `Please Reboot this machine`. Click on the `OK` button to close the window.

STEP 11: **Reboot the machine**. Select the `Reboot System` option from the `Hardware` pull-down menu. The `Reboot` dialog box appears with the following prompt: `Do you want to shutdown and reboot the computer?` Click on the `OK` button to reboot the machine.

NOTE: The system takes several minutes to reboot. During this time, several informational messages appear, including the following:

```
      NIS domainname is [domain name]
```

The domain name will be the name you specified in STEP 2. This message confirms that NIS has been initialized on the machine.

NOTE: The following message also appears on the master server ONLY upon this initial reboot:

```
      The password used will be nisplus
      Use this password when the nisclient script requests the network
      password.
```

This is the password to be entered in STEP 7 when NIS is initialized on the client machine.

When the reboot is complete, the DII COE Login window appears. NIS is configured.

Adding a NIS Client

Follow the steps below to add a machine as a NIS client.

> **NOTE**: NIS clients can only be added on the master server machine.
>
> **NOTE**: When adding a NIS client, the server and client must recognize each other through inclusion in the local hosts table.

STEP 1: **Select the `Add NIS Client` option**. Select the `Add NIS client` option from the `Set NIS` cascading menu option.

STEP 2: **Enter the client host name**. The `ENTER A RESPONSE` window appears. Enter the client host name at the prompt and click on the `OK` button.

STEP 3: **Enter the client IP address**. The `ENTER A RESPONSE` window appears. Enter the IP address at the prompt and click on the `OK` button.

STEP 4: **Enter and confirm the client root password**. The `ENTER A PASSWORD` window appears. Enter the root password and press [RETURN]. Re-enter the password to verify it and press [RETURN]. Then click on the `OK` button.

STEP 5: **Determine if you want to initialize the machine as a client**. The following prompt appears:

```
Initializing client [name] for domain “.”. Once
initialization is done, you will need to reboot your
machine. Do you wish to continue?
```

Type `Y` or `N` and press [RETURN]. The window closes.

STEP 6: **Reboot the machine**. Reboot the machine if you added a NIS client. Select the `Reboot System` option from the `Hardware` pull-down menu. The `Reboot` dialog box appears with the following prompt: `Do you want to shutdown and reboot the computer?`Click on the `OK` button to reboot the machine.

> **NOTE**: No message appears to tell you if the process was successful.

Removing NIS

The `Remove NIS` option deconfigures NIS from the system, which removes the domain name and, upon reboot, does not start NIS processes. Follow the steps below to disable and remove NIS.

STEP 1: **Select the `Remove NIS` option**. Select the `Remove NIS` option from the `Set NIS` cascading menu option.

STEP 2: **Disable and remove NIS**. The `ENTER A RESPONSE` window appears with the following message: `Do you wish to disable and remove NIS?` Click on the `No` button to close the window, or click on the `Yes` button to disable and remove NIS.

NOTE: No message appears to tell you if the process was successful.

STEP 3: **Acknowledge that the machine needs to be rebooted**. An informational message appears prompting you to reboot the machine. Click on the `OK` button.

STEP 4: **Reboot the machine**. Select the `Reboot System` option from the `Hardware` pull-down menu. The `Reboot` dialog box appears with the following prompt: `Do you want to shutdown and reboot the computer?` Click on the `OK` button to reboot the machine.

NOTE: The system takes several minutes to reboot. During this time, several informational messages appear, including the following:

```
NIS domainname is
```

This domain name field will be blank if NIS was removed successfully.

The system reboots to the DII COE Login screen.

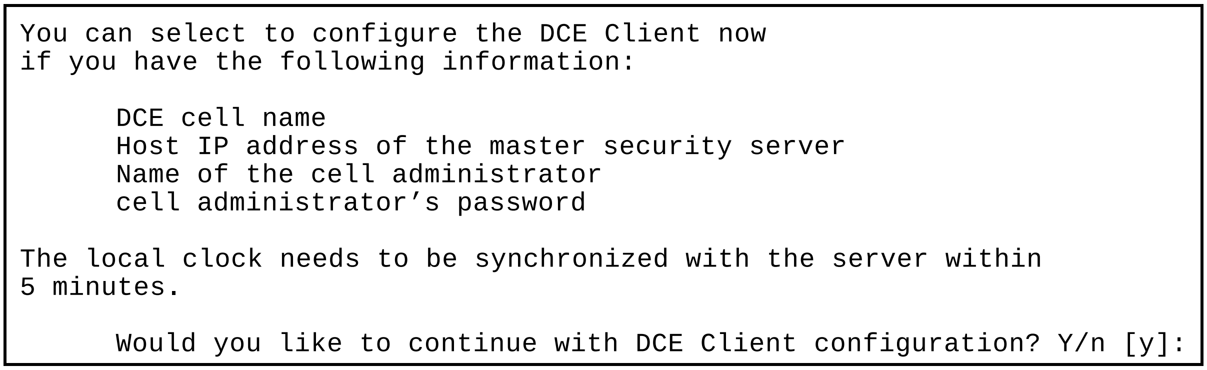
NOTE: If you want to enable NIS, reboot the workstation first, then initialize NIS.

6.4.5 DCE Option

The `DCE` option is a cascading menu that has four options: `Configure DCE Client`, `Configure DTS server`, `Configure Audit server`, and `Unconfigure DCE`. These options are described in the following subsections.

6.4.5.1 Configure DCE Client Option

The `Configure DCE Client` option allows the system administrator to configure a workstation as a client system in a DCE cell. Select the `Configure DCE Client` option to open the `DCE Client Configuration` screen (Figure 31).



```
You can select to configure the DCE Client now
if you have the following information:

      DCE cell name
      Host IP address of the master security server
      Name of the cell administrator
      cell administrator’s password

The local clock needs to be synchronized with the server within
5 minutes.

      Would you like to continue with DCE Client configuration? Y/n [y]:
```

Figure 31. DCE Client Configuration Screen

DCE is normally configured during initial system installation; however, DCE configuration can be skipped during the system installation process. Refer to the *DII COE Kernel Installation Guide (HP-UX 9.07)*, *DII COE Kernel Installation Guide (Solaris 2.4)*, or the *DII COE Kernel Installation Guide (Solaris 2.5.1)* for information about configuring the DCE client during initial system installation.

The `Configure DCE Client` option allows DCE client configuration to be performed after the initial installation. The interface is through a series of prompted questions and responses from a terminal window.

NOTE: The local clock *MUST* be synchronized to within 5 minutes of the server clock for the system to configure DCE. If the times are not synchronized, DCE configuration will fail.

NOTE: You must unconfigure DCE before attempting to configure DCE.

NOTE: Do not continue with the client configuration if a server is not configured and operating.

NOTE: If the system is configured into a cell, you must reconfigure the system before starting the DCE client configuration.

Follow the steps below to configure a workstation as a client system in a DCE cell.

STEP 1: **Determine if you would like to continue with the DCE client configuration**. Type `Y` or `N` at the prompt and press [RETURN].

STEP 2: **Enter the cell name**. Enter the cell name at the prompt and press [RETURN].

STEP 3: **Enter the Internet Protocol (IP) address of the master security server**. Enter the IP address at the prompt and press [RETURN].

STEP 4: **Enter the name of the cell administrator**. Enter the name of the cell administrator at the prompt and press [RETURN].

STEP 5: **Enter the cell administrator's password**. Enter the password at the prompt and press [RETURN].

STEP 6: **Determine if you would like to configure this node as a DFS client server**. Type `Y` or `N` at the prompt and press [RETURN]. If you are on an HP workstation, proceed to STEP 7; if you are on a Sun workstation, proceed to STEP 11.

STEP 7: **Determine where the cache is located**. The following prompt appears: `Is the cache: 1. in memory 2. on the local drive.`Type `1` or `2` and press [RETURN].

STEP 8: **Enter the size of the cache**. The following prompt appears: `Enter size of cache (10000)`. Enter a new cache size or press [RETURN] to accept the default value.

STEP 9: **Determine the cache directory**. The following prompt appears: `Enter the name of the cache directory (/opt/dcelocal/var/adm/dfs/cache)`. Enter a directory name or press [RETURN] to accept the default directory.

STEP 10: **Determine if the DFS client is to be configured as an NFS gateway**. The following prompt appears: `Would you like to configure this DFS client as an NFS gateway?`Type `N` and press [RETURN].

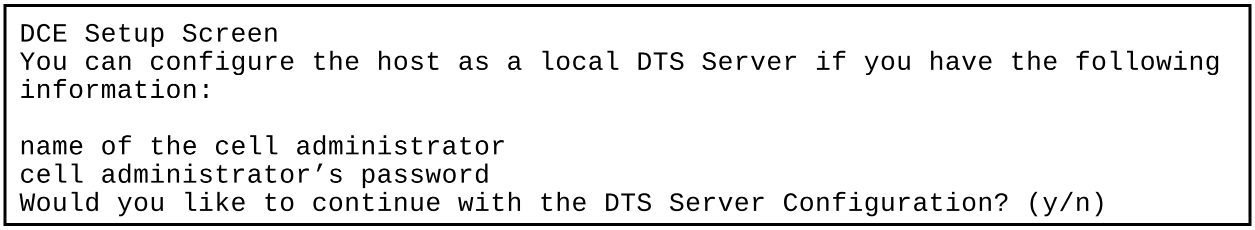
STEP 11: **Determine if you would like to configure this node as a local DTS server**. Type `Y` or `N` at the prompt and press [RETURN].

STEP 12: **Determine if you would like to configure this node as an audit server**. Type `Y` or `N` at the prompt and press [RETURN].

STEP 13: **Exit the DCE client configuration display**. Type `q` at the prompt and press [RETURN] to exit the DCE client configuration display.

6.4.5.2 Configure DTS Server Option

The `Configure DTS server` option allows the system administrator to configure the host as a local DTS server. Select the `Configure DTS server` option to open the `DCE Server Configuration` screen (Figure 32).



```
DCE Setup Screen
You can configure the host as a local DTS Server if you have the following
information:

name of the cell administrator
cell administrator’s password
Would you like to continue with the DTS Server Configuration? (y/n)
```

Figure 32. DCE Server Configuration Screen

Follow the steps below to configure the host as a local DTS server.

STEP 1: **Determine if you want to continue with the DTS server configuration**. Type `Y` or `N` and press [RETURN].

STEP 2: **Enter the name of the cell administrator**. Enter the name at the prompt and press [RETURN].

STEP 3: **Confirm the name of the cell administrator**. Enter the name again and press [RETURN].

STEP 4: **Enter the cell administrator’s password**. Enter the password at the prompt and press [RETURN].

STEP 5: **Exit the DTS server configuration display**. Type `q` at the prompt and press [RETURN] to exit the DTS server configuration display.

6.4.5.3 Configure Audit Server Option

Follow the steps below to configure the host as an audit server.

STEP 1: **Select the `Configure Audit` server option**. Select the `Configure Audit` server option from the `DCE` option cascading menu.

STEP 2: **Determine if you want to continue with the audit server configuration**. Type `Y` or `N` at the prompt and press [RETURN].

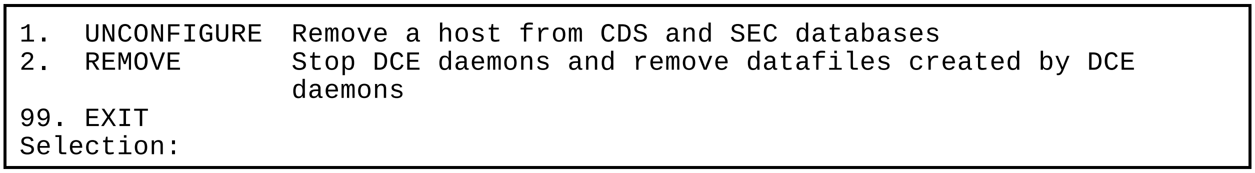
STEP 3: **Exit the audit server configuration display**. Type `q` at the prompt and press [RETURN] to exit the audit server configuration display.

6.4.5.4 Unconfigure DCE Option

The `Unconfigure DCE Client` option allows the system administrator to remove the system as a client from a DCE cell. The interface is through a series of prompted questions and responses from a terminal emulator window.

NOTE: Do not continue with the client configuration if a server is not configured and operating.

Select the `Unconfigure DCE Client` option to open the `DCE Setup` window (Figure 33).



```
1.  UNCONFIGURE  Remove a host from CDS and SEC databases
2.  REMOVE       Stop DCE daemons and remove datafiles created by DCE
                 daemons
99. EXIT
Selection:
```

Figure 33. DCE Setup Window

Follow the steps below to unconfigure the DCE client.

STEP 1: **Choose to unconfigure the DCE client**. Type `1` at the prompt and press [RETURN].

STEP 2: **Enter the cell administrator's account name**. Enter the cell administrator’s account name at the prompt and press [RETURN].

STEP 3: **Enter the password of the cell administrator**. Enter the password at the prompt and press [RETURN].

STEP 4: **Determine if you want to force unconfiguration**. Type `Y` or `N` at the prompt and press [RETURN].

STEP 5: **Exit the DCE client configuration display**. Type `q` at the prompt and press [RETURN] to exit the DCE client configuration display.

6.5 Removing Global Data

The `COERemoveGlobal` command line tool allows the system administrator to remove global segment data on the global users/profile workstation This should be done only if all segments referring this profile have been deinstalled. The specified segment must be available currently on the local workstation. When removing an Account Group segment, the whole directory will be removed (e.g., `h/USERS/global/Profiles/SampleAcctGrt`).

Follow the steps below to use the `COERemoveGlobal` command line tool.

STEP 1: **Log in as sysadmin**.

STEP 2: **Enter the appropriate password**. Enter a password for the sysadmin user.

STEP 3: **Open a terminal emulator window**.

NOTE: Command line tasks are performed in terminal emulator windows. Follow the steps below to access a terminal emulator window.

STEP 1: Double-click on the Application Manager control on the CDE Front Panel to open the `Application Manager` window.

STEP 2: Double-click on the `DII_APPS` folder in the `Application Manager` window to open the `Application Manager - DII_APPS` folder.

STEP 3: Double-click on the `SA_Default` folder to open the `Application Manager - SA_Default` window. This window contains both a `Dtterm` icon and an `Xterm` icon.

STEP 4: Double-click on either the `Dtterm` icon or the `Xterm` icon to open the window.

STEP 4: **Log in sysadmin**. Log in as sysadmin at the terminal emulator prompt.

STEP 5: **Enter the appropriate password**. Enter a password for the sysadmin user.

STEP 6: **Remove global data for the specified segment**. Type the following at the prompt:

```
COERemoveGlobal [flags] segment[RETURN]
```

NOTE: If you need help, type `COERemoveGlobal` without any parameters. The following message appears:

```
Usage: COERemoveGlobal [flags] segment
The usable flags are:
-h, h, ?:      Displays the help message
-V:      Displays the version number of the tool
-p <path>      Use path to reestablish path for subsequent filename
This tool will remove global data for the specified segment.
NOTE: If no Path is specified, /h will be used.
```

STEP 7: **Determine if global data has been deleted for the specified segment**. If the command was successful, the following message appears:

```
Successful Removal of Global Data for Segment [segment name]
```

If the command was not successful, the following message appears:

```
Unsuccessful Removal of Global Data for Segment [segment
name]
```

The prompt then reappears.

7. Security Administration Command Line Utilities

Two security administration tasks may be completed by using the command line: changing the security level of a workstation and auditing. These tasks are described in the following subsections.

7.1 Changing Workstation Security Levels

The `COESecLevel` command line tool can be used by the system administrator to change the security level of a workstation. Follow the steps below to use `COESecLevel`.

STEP 1: **Log in**. Log in as sysadmin.

STEP 2: **Enter the appropriate password**. Enter a password for the sysadmin user.

STEP 3: **Open a terminal emulator window**.

> **NOTE**: Command line tasks are performed in terminal emulator windows. Follow the steps below to access a terminal emulator window.
>
> STEP 1: Double-click on the Application Manager control on the CDE Front Panel to
> open the `Application Manager` window.
>
> STEP 2: Double-click on the `DII_APPS` folder in the `Application Manager` window to open the `Application Manager - DII_APPS`folder.
>
> STEP 3: Double-click on the `SA_Default` folder to open the `Application Manager SA_Default` window. This folder contains both a `Dtterm` icon and an `Xterm` icon.
>
> STEP 4: Double-click on either the `Dtterm` icon or the `Xterm` icon to open the window.

STEP 4: **Log in sysadmin**. Log in as sysadmin at the terminal emulator prompt.

STEP 5: **Enter the appropriate password**. Enter a password for the sysadmin user.

STEP 6: **Change the security level of the workstation**. Type the following at the prompt:

```
COESecLevel [security level][RETURN]
```

NOTE: If you would like a list of the security levels or need help, type `COESecLevel` without any parameters. The following message appears:

```
Usage: COESecLevel Security Level> is UNCLASS, CONFIDENTIAL, SECRET, TS,
       SCI.
```

(`TS` stands for top secret; `SCI` stands for sensitive compartmented information.)

STEP 7: **Close the terminal emulator window**. Type the following command at the prompt:

```
logout [RETURN]
```

STEP 8: **Reboot the system**. Select the `Reboot System` option from the `Hardware` pull-down menu. The `Reboot` dialog box appears with the following prompt: `Do you want to shutdown and reboot the computer?`Click on the `OK` button to reboot the machine.

STEP 9: **Log in as sysadmin or secman**. The security banner does not depend on the user.

STEP 10: **Enter the appropriate password**. The security banner will have changed to show the new security level.

7.2 Auditing

7.2.1 Auditing on Solaris

Enabling Auditing

Auditing on Solaris can be started automatically after initial kernel installation by typing `Y` at the following prompt: `This script is used to enable the Basic Security Module (BSM). Shall we continue with the conversion now (y/n)?` Refer to the *DII COE Kernel Installation Guide (Solaris 2.4)* or the *DII COE Kernel Installation Guide (Solaris 2.5.1)* for information on starting auditing automatically after initial kernel installation.

If auditing on Solaris was not started after initial kernel installation or has been disabled, auditing can be enabled by logging in as `root` and executing the shell script `/etc/security/bsmconv`, which configures the Basic Security Module.

NOTE: Auditing can only be enabled or disabled by the root user.

After the `bsmconv` command has been run, the system must be rebooted to initialize the auditing subsystem.

Disabling Auditing

Auditing is disabled by logging in as `root` and executing the shell script `/etc/security/bsmunconv`. The system must be rebooted after this script is executed.

7.2.2 Auditing on HP

Enabling or Disabling Auditing From SAM

NOTE: Refer to vendor documentation for more information on using SAM.

Follow the steps below to start or stop audit from SAM.

STEP 1: **Invoke SAM**.

STEP 2: **Select the `Auditing and Security` option**.

STEP 3: **Select either the `Users`, `Events`, or `System Calls` option**.

STEP 4: **Convert to a trusted system**. The following message appears:

```
You need to convert to a Trusted System before
proceeding. The conversion process does the following
things:

1.    It saves a copy of "/etc/passwd" in the file
      "/etc/passwd.old.sav".
2.    It then moves the passwords from "/etc/passwd"
      into a new "hidden" password database (the file
      "/.secure/etc/passwd").
3.    It invalidates all passwords in "/etc/passwd" by
      replacing them with "*".  For more details,
      refer to the "HP-UX System Security" manual.

            Do you wish to convert to a Trusted System
            now?
```

Click on the `Yes` button.

STEP 5: **Affirm that you want to convert to a trusted system**. The following message appears:

```
WARNING:   The change to a Trusted System is
           irreversible!  Are you sure you want to
           continue?
```

Click on the `Yes` button.

STEP 6: **Finish with the conversion**. The following message appears:

```
Converting to a trusted system ...
Task succeeded.  Press OK to continue.
```

Click on the `OK` button.

STEP 7: **Turn auditing on or off.** Select either the `Turn Auditing Off` or `Turn Auditing On` option from the `Actions` button on the menu to stop or start audit, respectively.

Using Shadow Password Files

To use a shadow password file on HP, type `/etc/tsconvert`. This utility updates the shadow password file and removes all password information from the default password file. Once this program has completed, the machine must be rebooted.

To discontinue use of a shadow password file on HP, type `/etc/tsconvert -r`. This utility restores the default password file with the actual encrypted password information. Once this program has completed, the machine must be rebooted.

8. Error Recovery Guidelines

NOTE: Never power off the system without first executing a shutdown. Doing so could cause irreparable damage. If the system has already been brought down incorrectly, refer to Subsection 8.4, *Repairing File Systems*.

The following topics are covered:

C Recovering from basic errors

C Troubleshooting multiple monitors

C Identifying hardware problems

C Repairing file systems

C Reporting problems.

8.1 Recovering From Basic Errors

Access to all System Administration menus and options is required to perform error recovery procedures.

> **IMPORTANT**! The following procedures are listed according to "risk factor"—that is, from the least to the greatest risk of damaging files or losing data. Always begin corrective action with the procedure that poses the least risk.

If these steps do not correct the problem, contact the number listed in Section 8.5, *Reporting Problems*.

Options are unavailable:

C Access to options may be restricted for the user's account. Check with the security manager.

Window hangs or menu option has been disabled:

C Select the `Close All` option from the `SA System` pull-down menu (on the System Administration menu bar). All windows launched from the menu bar or from the `DII_APPS` folder will close. Windows launched from the CDE front panel will not close.

Reboot the system:

STEP 1: Notify users on remote monitors that their applications will soon terminate.

STEP 2: Select the `Reboot System` option from the `Hardware` menu on the System Administration menu bar.

STEP 3: Restart the system with user login.

Power up/power down the system with pointer and keyboard operational:

C See Chapter 3, *Operating Guidelines*.

Power up/power down the system with pointer frozen:

STEP 1: Turn off the monitor and peripherals.

STEP 2: Turn off the CPU.

STEP 3: Wait approximately 30 seconds.

STEP 4: Turn on the monitor and peripherals.

STEP 5: Turn on the CPU.

STEP 6: Restart the system with the user login.

Reinstall the DII COE:

STEP 1: Use the original installation tapes if a network installation is not possible.

STEP 2: Follow the instructions to reinstall the DII COE.

8.2 Troubleshooting Multiple Monitors and Keyboards

Monitor or keyboard fails to respond:

C A reboot may solve the problem.

C Rebooting the computer in a multiple monitor environment means all monitors will go down. When working with multiple monitors, contact all users before rebooting.

Monitor is black:

C Make sure the monitor cable is connected properly.

C Make sure the monitor is connected to a power supply and is turned on.

C The video switch may have incorrect input or output, or may be turned off.

Monitor is black with small yellow squares (HP only):

C Make sure each monitor is connected to the correct port on the back of the CPU.

Second monitor in a dual-eye configuration is gray:

C Make sure keyboards are connected correctly. This monitor is the second eye of a dual-eye configuration.

Trackball does not respond:

C Reboot the machine. If this does not work, try using a different trackball. If the trackball still does not respond, there may be a wiring problem in the cable.

Keyboard does not respond:

C Make sure the keyboard is connected properly.

C The keyboard may be connected properly but the monitor may not "echo" the typed characters to the screen. Rebooting the machine usually solves this problem.

8.3 Identifying Hardware Problems

When the workstation is turned on, the CPU runs a hardware check. If the hardware check is successful, the following occurs:

C The system boots from the default boot device.

C The system displays configuration information, followed by the login prompt.

C Observe the boot information for system/hardware problems. If the boot fails, a disk problem has occurred. Refer to the hardware manual for more information.

8.4 Repairing File Systems

If the system was brought down unexpectedly (e.g., power failure, turned off without proper shutdown), it is designed to repair the file system when powered up.

C The system should never be powered down while the file system is being repaired. To do so would cause further damage to the file system.

C If power is fluctuating, leave the system off until power is re-established.

8.5 Reporting Problems

To receive immediate assistance with a problem or to report a problem, call the DII COE hotline at (703) 735-8682 between the hours of 9:00 a.m. to 5:00 p.m. Eastern Standard Time. The hotline is located at the Operational Support Facility (OSF) in Sterling, Virginia.

If a problem cannot be corrected by the procedures described in this document, follow these guidelines to report it:

STEP 1: **Make sure the problem can be repeated**.

STEP 2: **Record pertinent information**. Record the problem, the last steps leading to the problem, and the frequency with which the problem occurs.

STEP 3: **Describe attempts to solve the problem**.

Appendix A - Communications

A.1 The DII COE Network

An HP or a SPARC loaded with the DII COE can be configured as a stand-alone machine or networked in a server/client relationship.

A.1.1 Stand-alone Configuration

A stand-alone machine is its own server. It retains data without relying on a networked server. It shares data (1) through messages transmitted over configured comms ports or (2) by floppy diskette or tape.

A.1.2 Network Configuration

The communications processor holds all track and comms data. When installing software, the communications processor should be installed first, followed by its client machines. Client machines depend on the server for data, especially data from the track database. Communications processor functions include:

C Processing incoming and outgoing messages

C Decoding incoming messages

C Correlating track information

C Routing outgoing messages.

If the server goes down, the Track Database Manager (Tdbm) warning window informs the user that the server is down. Although the user can view track information, no track database actions (local or shared) are processed.

A.2 Interface Description

The DII COE supports two interface types: serial and LAN.

A.2.1 Serial Interface: RS-232, RS 422, MIL-188

A serial interface is used for serial communication between systems. If systems are at the same site, connect them directly. If systems are at different sites, connect them through a secure modem, such as a STU III.

A.2.2 LAN Interface: Ethernet and Fiber Optic Cabling

Ethernet and fiber optic cabling are used to enable communications between two or more workstations on a LAN. Each machine is assigned a unique name and IP address on the network, which are used by system files.

A.2.3 Protocols

A.2.3.1 TCP/IP

Transmission Control Protocol (TCP) moves data in a continuous, unstructured byte stream. It provides full-duplex service, acknowledgment of data received, and data flow control.

Internet Protocol (IP) provides network layer services to the TCP/IP protocol suite. IP is responsible for forwarding packets through a network based on IP addresses. IP relies on TCP to guarantee delivery of packets.

A.2.3.2 X.25

X.25 is used for a Wide Area Network (WAN) of computers connected by a Packet Switching Network (PSN), such as the Defense Data Network "DSNET1". (X.25 is generally used by ashore sites only.)

A.3 Physical Connections

A.3.1 Serial

A.3.1.1 Requirements for a Direct Connection

A 2-, 3-, and 7-pin connection is required to connect systems located in the same installation.

A.3.1.2 Requirements for STU III Connection

The STU III must support an RS-232 connection. If it does not, the user must request an RS-449-to-RS-232 adapter from the manufacturer.

An HP workstation requires a DB 9 female-to-DB 25-male cable. Certain models of STU III require voltage on pins 4 and 20, which the HP workstation does not supply. A special adapter must be used.

A.3.2 LAN

A.3.2.1 Requirements for an Ethernet Interface

C Use an AUI interface with a DB 15-pin connector between the workstation and the transceiver.

C The copper LAN interface may have a BNC connection between transceivers.

C The network must be terminated at both ends. Use a terminating 50W resistor on each end.

C If the workstation is a stand-alone configuration, the LAN connections on the workstation must be terminated. Use a 50W resistor on each end.

A.3.2.2 Requirements for a Fiber Optic Connection

C Use an AUI interface with a DB 15-pin connector between the workstation and the transceiver.

C The transceiveres must reside at each computer connected by fiber optics. These boxes have dual-ring capability to ensure continued transmission.

For example, if a transmission is interrupted by a broken fiber optic or connection, it is automatically routed to the second ring.

A.3.3 X.25

Requirements for an X.25 Connection (HP)

C If the system is configured for DDN communications, the Serial A port must be the DDN/X.25 interface device. No other device may be configured to the TTYA port.

C A DB 15 connects the machine to a modem and encryption device with an X.25 interface.

C The X.25 card provides synchronous RS-232 (DTE) error-free transmission over the PSN.

C There may be many interfaces, such as crypto, modem, or leased line, between the computer and the actual PSN.

A.4 Communication and Broadcast Configuration

Modify fields to configure a communications channel. Keep in mind the following general information:

C Standard comms settings should be used. Changing some settings, such as baud rate, parity, or stop bits, may cause data to be garbled. For example, if messages are garbled, it is likely that the transmitting and receiving sites do not have the same values set for the baud rate and related fields.

C XON/XOFF should never be used for baudot data connections. Toggle on the `XON/XOFF` checkbox to enable the use of software flow control to stop and resume transmission.

C If the `RTS/CTS` checkbox is toggled on, hardware flow control is enabled.

C Make sure the comms interface configuration matches the flow control settings.

A.4.1 Starting Comms Channels

A comms channel must be turned on before it can be used.

Turn channels on and off one of two ways:

C Highlight the channel and then select `START`, `STOP`, or `RESTART` from the pop-up menu.

C Toggle the `AUTOSTART` checkbox `ON` in the `COMMS EDIT` window. This turns a channel on at system startup.

The `STATUS` column indicates status of each channel: `ON` or `OFF`.

Important:

C A comms channel can only be turned on if the designated device exists. For example, a DTC comms channel is assigned to TTYC2. If a multiplexer is not connected to the TTYC port, this channel cannot be turned on, but it can be reassigned to an existing port.

C A channel must be `ON` to open its status window.

Highlight the channel and select the `WINDOW` pop-up option.

A.4.2 Starting Broadcasts

A broadcast must be turned on before it can be used. Broadcasts are turned on and off using the `BROADCASTS` option from the `FOTC/BCST` menu. The `BROADCASTS` window displays a list of available broadcasts.

Turn broadcasts on and off one of two ways:

C Highlight the broadcast; select `START` from the pop-up menu.

C Toggle the `AUTOSTART` checkbox `ON` in the `BROADCAST EDIT` window. This turns the broadcast on at system startup.

The `STATUS` column indicates status of each broadcast: `ON` or `OFF`.

A.4.3 Message Transmission

Messages are sent manually (using an `XMIT` option) and automatically (using a broadcast). To transmit a message, make sure the communications channel is turned on, the channel is configured properly, and the channel can transmit messages.

NOTE: Manual transmissions are not allowed on the DTC channel; only automatic transmissions are allowed via the DTC broadcast.

To broadcast a message, make sure the appropriate comms channels are running, as described in the previous section, and the appropriate broadcast programs are running, as described below.

A.4.4 Message and Broadcast Headers

To set a default message header for manual transmissions, click `DEFAULT` in the `HEADER EDIT` window pop-up menu. This header is used for all options that have a manual transmit capability, such as tracks and overlays.

Each broadcast has its own header. If `DEFAULT` is selected while creating a header for a broadcast, the broadcast header becomes the default message header. This header is used for manual transmissions and for the broadcast.

A.5 STU III Configuration

A serial interface comms channel must first be configured for the STU III connection (see Section A.3, *Physical Connections*). Set the device to the port connected to the STU III. Use serial interface defaults for the other settings: `data type=ASCII`, `parity=NONE`, `stop bit=1`, `baud rate=2400`, `data size=8`, `RECV` and `XMIT=ON`.

C An entry must be made in the Auto-Forward Table. (See *Auto-Forward Table* in the *Unified Build User's Guide*.)

C An entry must be made in the Sources reference table if in FOTC mode. (See *Source XREF Table* in the *Unified Build User's Guide*.)

C Both STU IIIs must be in Remote Control Mode with Secure Access Control System (SACS) enabled.

C Both STU IIIs must have proper ACLs loaded.

C STU IIIs with SACS support auto-answer auto-secure-no operators are needed. In this mode, Voice/Secure Voice options are unavailable.

SACS grants access to designated STU IIIs, as identified in the ACL on the local STU III.

Three requirements for secure authentication of automatic, incoming calls are (1) ACL header, (2) DAO code, and (3) Keyset ID.

STU IIIs (including STU III SACS) without these codes are excluded, and cannot gain access or connect with STU-IIIs that share DAO codes or keyset IDs.This creates a closed network. Unauthorized calls are disconnected before the line to JMCIS is opened. If two STU IIIs can talk to each other, but cannot transmit data, their internal modes may be different. Check baud rates: synchronous and asynchronous must match.

A.5.1 Downloading ACL

The following tables illustrate the sequence of an ACL download. This sequence has been tested on AT&T devices only.

STEP 1: Insert the Master CIK.

STEP 2: Click on the `MENU` option.

OBSERVE	PRESS
`Main Menu Secure Voice`	`NEXT`
`Main Menu Secure Data`	`NEXT`
`Main Menu Show Config`	`NEXT`
`Main Menu Change Config`	`SELECT`
`Change Config Security Config`	`SELECT`
`Security Config SACS Disable`	`NEXT`
`Security Config SACS Options`	`SELECT`
`SACS Options SACS Control`	`NEXT`
`SACS Options Auto Access Control`	`NEXT`
`SACS Options Far-end ID`	`NEXT`
`SACS Options Access List`	`SELECT`
`ACCESS LIST MENU Load ACL Via DTE`	`SELECT`
`WAITING FOR ACL start DTE transfer`	(begin download)
`RECEIVING ACL please wait`	(wait until finished)
`ACL RECEIVED nnn show new ACL`	`NEXT`
`ACL RECEIVED nnn save new ACL`	`SELECT`
`NEW ACL SAVED previous menu`	`MENU`

A.5.2 Temporarily Disabling SACS ACL

STEP 1: Insert the Master CIK.

STEP 2: Click on the `MENU` option.

OBSERVE	PRESS
`Main Menu Secure Voice`	`NEXT`
`Main Menu Secure Data`	`NEXT`
`Main Menu Show Config`	`NEXT`
`Main Menu Change Config`	`SELECT`
`Change Config Security Config`	`SELECT`
`Security Config SACS Disable`	`SELECT`
`SACS Disable on/off change Disable`	`SELECT`

A.5.3 Autodialing Between Two AT&T STU IIIs

STEP 1: Insert the Master CIK.

STEP 2: Click on the MENU option to turn auto-answer on.

After the ACL is downloaded, but before it is put in Remote Control Mode, auto-answer must be on.

If the display indicates one or more AASD rings, auto-answer is on.

PRESS	PRESS
NEXT until "Change Config"	SELECT
NEXT until "Security Config"	SELECT
NEXT until "SAC Options"	SELECT
NEXT until "SACS Control" (ensure SASCTRL is enabled.)	SELECT

PRESS	PRESS
MENU	MENU (again)
NEXT until "Change Config"	SELECT
NEXT until "Security Config"	SELECT
The display panel will read SACS Disable (ensure SACS Disable is OFF)	SELECT

PRESS	BUTTON
MENU	MENU (again)
NEXT until "Change Config"	SELECT
NEXT until "Security Config"	SELECT
NEXT until "SAC Options"	SELECT
NEXT until “Auto Access Ctrl”	(Ensure Auto Access Ctrl is ON)

PRESS	BUTTON
MENU	MENU (again)
NEXT until"Change Config"	SELECT
NEXT until "Auto-Answer"	SELECT

A.5.4 Configuring Specific STU-III Models

Motorola SECTEL 1000/2000:

C This device provides the auto-secure feature, but does not allow auto-answer, nor does it support SACS.

C The default data mode is 2400 baud, asynchronous.

C An RS-232 port is included, allowing direct connection to the system.

C A serial communications interface must be used.

RCA STU III:

C The STU III data port is an RS-232 (DB 25) or an RS-449 (DB 37) connection, depending on manufacturer and model.

C RS-232 and RS-449 share the same signal levels but have a different pinout.

C RS-449 ports must be converted to RS-232 to work with the system. These converters are included with the STU III.

The following table illustrates the conversion requirements of a STU III RS-449 configuration to an RS-232.

Table 1. RS-449 to RS-232 Conversion

RS-449 (STU-III)	**RS-232 (TDP)**
1–Shield	1–Shield
4–Send Data (+)	2–TXD
6–Receive Data	3–RXD
7–Request to Send	4–RTS
9–Clear to Send	5–CTS
11–Data Mode	6–DSR
19–Common Return	7–Common
20–Receive Common	
22–Send Data (-)	
37–Send Common	
12–Terminal Ready	20–DTR

Follow the steps below to configure an RCA STU III:

STEP 1: Press `PROGRAM`.

STEP 2: Press `SETUP`.

STEP 3: Press `YES` at "`set terminal options`."

STEP 4: Press `YES` at "`set standard options`." The standard settings are:

- Dialing mode: TONE
- Comm mode: FULL DUPLEX
- Data Ports: 2400 ASYNC
- Remote Capable: DISABLED
- A-lead Control: ENABLED
- Dual Home: Line 1 only.

Appendix B - Multiple Monitor and Keyboard Configurations

A single, properly equipped HP TAC-3 (Tactical Advanced Computer) CPU can drive any of the following configurations:

C Single-eye console with 1-3 single-eye remote monitors

C Dual-eye console with 1-2 single-eye remote monitors

C Dual-eye console with a dual-eye remote monitor.

Tables 2 and 3 illustrate the recommended single-eye and dual-eye monitor connection schemes. For potential difficulties the user may encounter in a multi-monitor environment, see Subsection 8.2, *Troubleshooting Multiple Monitors and Keyboards*.

Table 2. Single-eye Console

Single-eye Console	**Remote 1**	**Remote 2**	**Remote 3**
Monitor: crt00 Keyboard: KYBD4	None	None	None
Monitor: crt00 Keyboard: KYBD1	**Single-eye** Monitor: crt01 Keyboard: KYBD2	None	None
Monitor: crt00 Keyboard: KYBD1	**Single-eye** Monitor: crt01 Keyboard: KYBD2	**Single-eye** Monitor: crt10 Keyboard: KYBD3	None
Monitor: crt00 Keyboard: KYBD1	**Single-eye** Monitor: crt01 Keyboard: KYBD2	**Single-eye** Monitor: crt10 Keyboard: KYBD3	**Single-eye** Monitor: crt11 Keyboard: KYBD4

Table 3. Dual-eye Console

Dual-eye Console	**Remote 1**	**Remote 2**
Top Monitor: crt01 Bottom Monitor: crt00 Keyboard: KYBD1	None	None
Top Monitor: crt01 Bottom Monitor: crt00 Keyboard: KYBD1	**Single-eye** Monitor: crt10 Keyboard: KYBD4	None
Top Monitor: crt01 Bottom Monitor: crt00 Keyboard: KYBD1	**Single-eye** Monitor: crt10 Keyboard: KYBD3	**Single-eye** Monitor: crt11 Keyboard: KYBD4
Top Monitor: crt01 Bottom Monitor: crt00 Keyboard: KYBD1	**Dual-eye** Top Monitor: crt11 Bottom Monitor: crt10 Keyboard: KYBD3	None

Appendix C - Database Size Limits

This appendix lists database limits for various DII COE files.

Table 4. Track Limits

Tracks	Limits
Platform/Ambiguity	1500
Emitter	1500
Link	1024
Acoustic	100
Unit	500
SI	450
External	0

Table 5. Other Track Range Limits

Other Track Ranges	Limits
Confidence Level of AOU Cross-fix Ellipse	90 percent
Dynamic Status Board	1 master track / 20 slave tracks
Land Sites	100
Missile Systems/Track	10
Radar Systems/Track	10
Sonar Systems/Track	10
Weapon Systems/Track	10
Specific IFF Mode-2 Valued Tracks Can Be Archived	20
Track Archive Sequence of Steps	60 seconds
Track Groups	32
Tracks/Group	Limited only by disk storage
Track History Reports/Track	1,000
Track Symbol Label	26 characters

Table 6. Communications Limits

Communications	**Limits**
Addressee (Channel Message Buffer Manager)	1,000 backlog messages
Alert Log	1,000 messages
Incoming Message Log	1,000 messages
Incoming Opnote Log	200 opnotes
Outgoing Message Log	1,000 messages
RAINFORM Messages	1,000 lines
Received Messages Displayed in Status Window	1,000 messages
Report Log	2,000 reports
Saved for Raw Messages	500 lines

Table 7. Miscellaneous Limits

Miscellaneous	**Limits**
Auto-Forwarding, Addresses	500
Broadcast, User-Set Cycle Rate	0-720 minutes
Broadcasts, Active	25
Characters Stored per Screen Name	50
Clipboard, Files Stored on	1,000
Engagement Scenarios	10
Grid Cells, Number of	24 or 48
IFF/DIs, Nicknames	100
Incoming Message Alert, Addresses	5
Incoming Message Alert, Originators	5
Net Address (DDN)	256
Satellite Charlie Elements	300
Satvul-Satellites per Category	300
Stored Screen, Briefing Slides	50
Stored Screens, Number of	50

Table 8. Map Limits

Maps	**Limits**
Key Sites	1,000
Stored Map, Parameter Combinations	500
Stored Maps	20
Zoom Width, Greatest	21,600 NM
Zoom Width, Smallest	0.25 NM

Table 9. Overlay Limits

Overlays	**Limits**
Overlay, Items	100
Overlay, Points	256
Overlay, Polyline Points	256
Overlays, Number of	500

This page intentionally left blank.

Part 2. Profile Based Account Management Guide for Users and System Administrators

Preface

The following conventions are used in this document:

Bold	Used for information that is typed, pressed, or selected in executables and instructions. For example, select **connect to host**.
Italics	Used for file names, directories, scripts, user IDs, document names, Bibliography references, and unusual computerese the first time it is used in text.
Underline	Used for emphasis.
Arrows <>	Used to identify keys on the keyboard. For example <Return>
"Quotation Marks"	Used to identify informal, computer-generated queries and reports, coined names, and to clarify a term when it appears for the first time. For example "Data-Generation Report."
`Courier Font`	Used to denote anything as it appears on the screen or commands. For example `tar xvf dev/rmt/3mm`
Capitalization	Used to identify keys, screen icons, screen buttons, field, and menu names.

1. Introduction

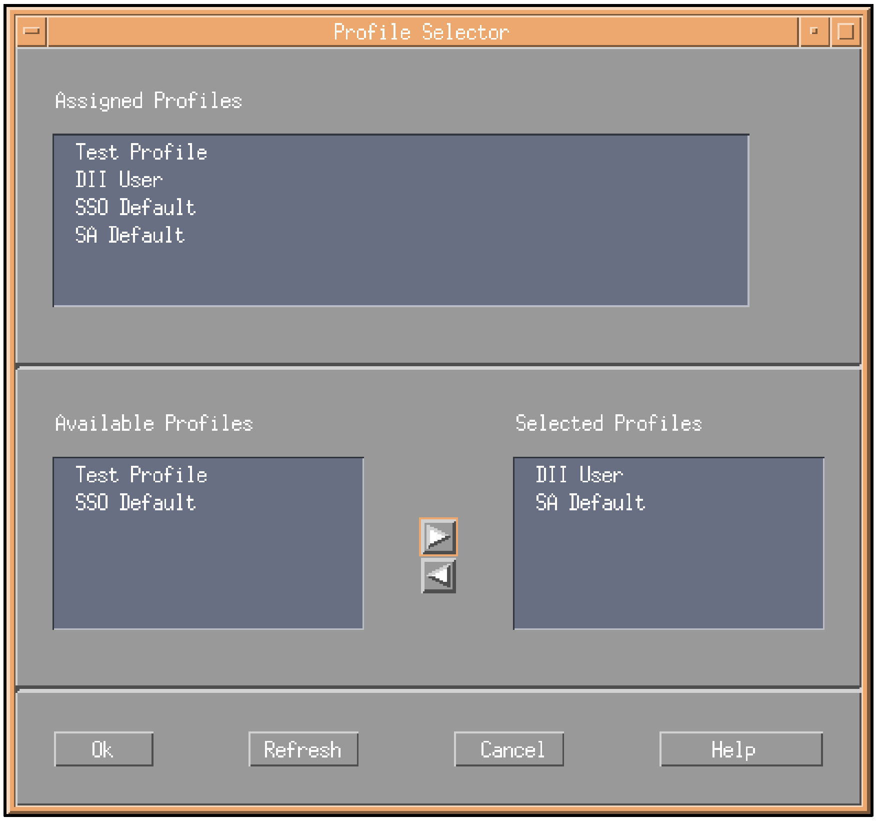
This guide provides information on the profile-based user access features of the Defense Information Infrastructure (DII) Common Operating Environment (COE). The information is presented in three parts. Section 2 is intended for the DII COE end-users, those who use the various applications and databases available through the DII COE interface in the course of their daily jobs whether they be planning staff members at a Global Command and Control System (GCCS) site, logisticians working on a Global Combat Support System (GCSS) project, or part of a deployed task force. Sections 3 and 4 are for the System Administrators (SA) and Information System Security Officers (ISSO) who are responsible for the overall administration and management of the DII COE, and for insuring that the system is configured and maintained in strict accordance with the security policies and procedures.

Profile Management is accomplished through use of the Security Manager and Edit Profiles software in the DII COE kernel, which provide a set of services for managing user accounts and associated permissions. A part of account management is controlling a user's access to system functions and components and this is accomplished by building "profiles" for the users or groups of users. These profiles are collections of applications and other system functions which an individual user or group of users need to perform a given job or role. If an individual performs different tasks at different times, multiple profiles can be constructed for the various tasks or the SA may choose to include all of the necessary applications and functions in one profile to maintain a single user to single profile relationship.

2. User Information

2.1 Profile Selector Overview

As a DII COE user, your involvement with Profile Management does not need to be extensive or complicated. Your primary interest is to get the information and applications that you need as quickly and effortlessly as possible and this is one of the things that Profile Management is designed to accomplish. In fact, depending on the system configuration of your particular site, you might not even be aware that it exists at all. This is because of the option available to your SA whereby each user is assigned only one profile containing access to all of the system features that you need. If this is the way your local system is set up, then after logging on, you will see a desktop containing icons for everything that you need and the fact that Profile Management put them there for you is largely irrelevant. At most sites however, and especially the larger ones, it is likely that you will have access to multiple profiles. Each of these profiles will be tailored for you to fit a particular role or position that you might occupy. When this system configuration is in use, you will be presented with the Profile Selector dialog box (see Figure 2-1) after logon. This allows you to select the profile that you need to accomplish the tasks at hand.



Profile Selector

Assigned Profiles

Test Profile
DII User
SSO Default
SA Default

Available Profiles

Test Profile
SSO Default

Selected Profiles

DII User
SA Default

Figure 2-1. Profile Selector Dialog Box

2.2 Choosing Profiles

The top section of the Profile Selector dialog box is the Assigned Profiles. This section shows valid profile(s) for that specific user. The bottom left section is the Available Profiles. This section shows the user's currently available but not selected profile(s). The bottom right section is the Selected Profiles. This section shows the user's currently selected profile(s). There are four buttons at the bottom of the window: "OK," "Refresh," "Cancel," and "Help." Their use will be explained later. To select a profile(s) that you want to use, highlight the profile(s) in the Available Profiles section and click on the **arrow** button that points to the Selected Profiles section. The profile(s) you have selected are now listed in the Selected Profiles section. If these are the profiles you will be using, click on the **OK** button at the bottom left of the dialog box.

To deselect a profile(s), highlight the profile(s) in the Selected Profiles section and click on the **arrow** button pointing left, to the Available Profiles. The profiles that you have deselected are now listed in the Available Profiles section. If these are the profiles you will not be using for a while, click on the **OK** button.

Should you need to change from one profile to another of those that are assigned to you during your working session, you can get to the Profile selector without having to logout. Just click on the **Profile Selector** icon (see Figure 2-2). This icon looks like the profile of a human with a big question mark.

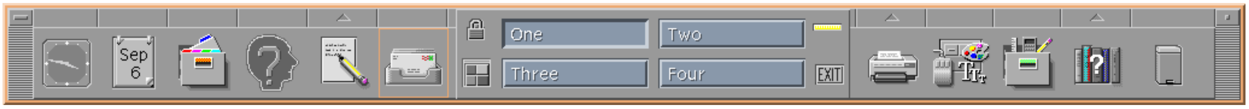
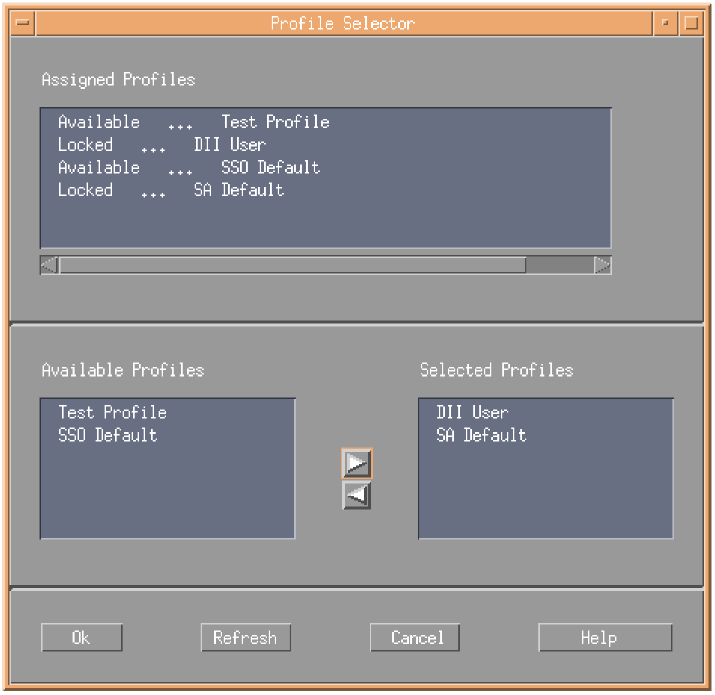


Figure 2-2. Main Control Panel

2.3 Profile Site Options

There is another site configuration option that you should be aware of and that is the "locked profile mode." This feature allows the SA to lock a profile thereby making it available to only one user at a time. If you try to select a locked profile that is already in use, you will get an error message even if it is one of your assigned profiles. Figure 2-3 shows another view of the Profile Selector dialog box, this time on a system employing the profile locking mode.



```
Available  ...  Test Profile
Locked  ...  DII User
Available  ...  SSO Default
Locked  ...  SA Default
```

Figure 2-3. Profile Selector - Control Option

Notice that the top window, "Assigned Profiles," contains slightly different information. The profiles listed are the same but now the names are preceded with the notation "Available" or "Locked." Only the SA or the security officer can alter the locking feature so you must contact one of them if you need immediate access to a locked profile, unless you know who else is using it. If the user will deselect the profile that you need, you will be able to select it by using the Refresh button. This button is used only on systems configured for the Locked Profile Mode and is otherwise inactive. Clicking on it after another user has de-selected a locked profile will cause the profile to be available to you on your Profile Selector. The Cancel button will terminate the profile selection session, returning the screen to the same state that it was in when the session was opened. The Help button will bring up the Profile Selection Help window.

3. SA and ISSO Information

3.1 Starting Security Manager

Only those user accounts which are assigned to profiles under the Security Admin account group may run Security Manager. Follow the steps below to access DII COE security administration functionality:

Step 1: Login as secman.

Step 2: Enter the appropriate password.

Step 3: Double-click on the **Application Manager** icon on the CDE Main Control Panel. Refer to Section 5 of the *DII COE System Administrator's Guide (HP and Solaris)* for more information about CDE.

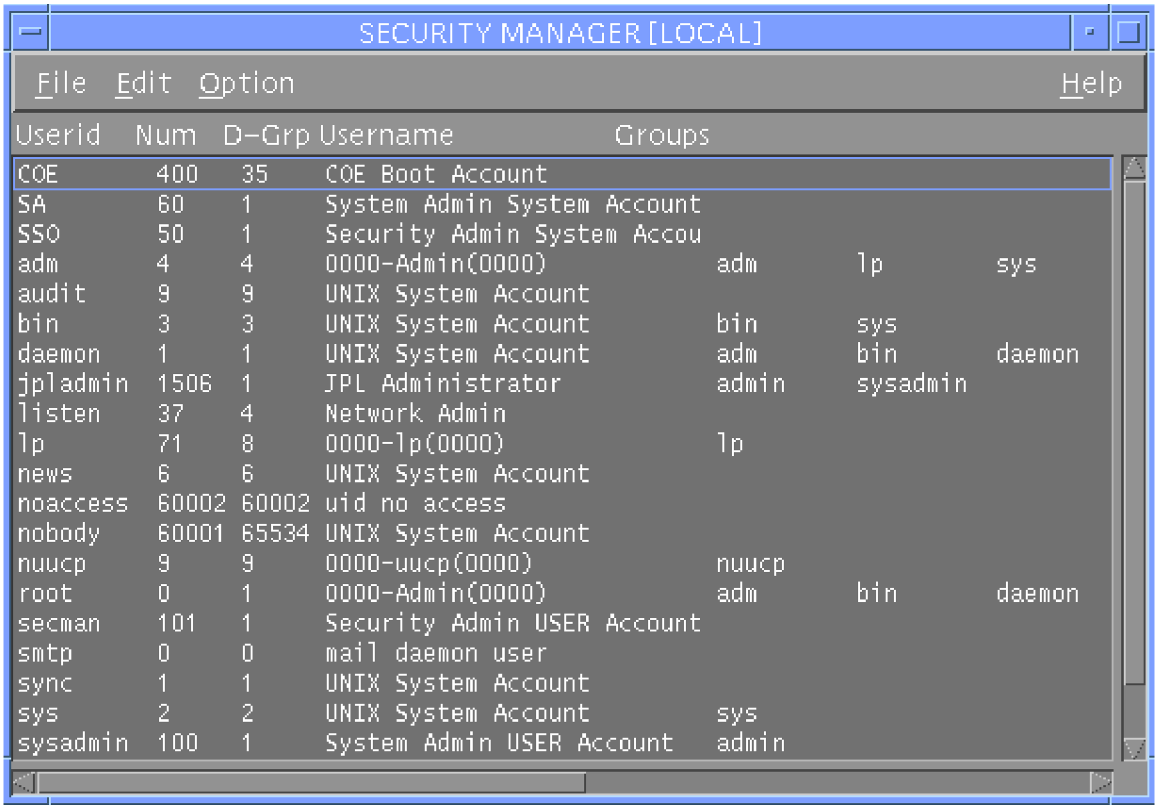
Step 4: Double-click on the **DII_APPS** icon. The Application Manager - DII_APPS window appears.

Step 5: Double-click on the **SSO_Default** icon. The Application Manager - SSO_Default window appears. This window displays a list of all user accounts.

Step 6: Double-click on the **Security Manager** icon. The SECURITY MANAGER [LOCAL] window appears (see Figure 3-1).

3.1.1 Security Manager Window

The scope of the current session is shown in brackets after the SECURITY MANAGER window name. The default scope is local so the sample window is named SECURITY MANAGER [LOCAL]. Paragraph 3.2 gives instructions for selecting the scope of the accounts that you plan to work on during your current session and for changing the scope during a session.



```
Userid    Num   D-Grp Username                 Groups
COE       400   35    COE Boot Account
SA        60    1     System Admin System Account
SSO       50    1     Security Admin System Accou
adm       4     4     0000-Admin(0000)         adm      lp       sys
audit     9     9     UNIX System Account
bin       3     3     UNIX System Account      bin      sys
daemon    1     1     UNIX System Account      adm      bin      daemon
jpladmin  1506  1     JPL Administrator        admin    sysadmin
listen    37    4     Network Admin
lp        71    8     0000-lp(0000)            lp
news      6     6     UNIX System Account
noaccess  60002 60002 uid no access
nobody    60001 65534 UNIX System Account
nuucp     9     9     0000-uucp(0000)          nuucp
root      0     1     0000-Admin(0000)         adm      bin      daemon
secman    101   1     Security Admin USER Account
smtp      0     0     mail daemon user
sync      1     1     UNIX System Account
sys       2     2     UNIX System Account      sys
sysadmin  100   1     System Admin USER Account  admin
```

Figure 3-1. Security Manager Main Window

Security Manager displays user account information in the main window. Accounts will be listed by user name, numeric ID, the numeric ID of the default group to which the account belongs, the name of the account, and any additional groups to which the account has access.

The SECURITY MANAGER window has the following fields:

Userid: User name.

Num: User ID number assigned to the user by the system.

D-Grp: Default account group number to which the user belongs; assigned by the system.

Username: Description of the account.

Groups: Groups to which the user belongs.

The SECURITY MANAGER window has three pull-down menus: File, Edit, and Option. These menus and their associated options are described in Paragraphs 3.1.2, 3.1.3, and 3.1.4.

3.1.2 File Menu

The File menu contains options to create and delete accounts, create and delete groups, edit a particular user's groups, edit a particular group's users, add and delete profiles, assign applications to profiles, and assign profiles to users. The File menu has the following options: Create Account, Delete Account, Groups, Profiles, and Exit. These options are discussed in Subsections 3.3 (Accounts), 3.4 (Groups), and 3.5 (Profiles). Exit closes Security Manager.

3.1.3 Edit Menu

The Edit menu contains options to cut, copy, and paste selected text from one field to another, as well as to delete selected text. Text can be cut, copied, pasted, or deleted from any text field that requires user input in any user window. To use the Cut option, use the mouse to highlight the text you want to cut from a text input field in a user window, then select **Cut** from the Edit pull-down menu in the SECURITY MANAGER window. The text that was cut will no longer appear in the text input field. To use the Copy option, use the mouse to highlight the text you want to copy, select **Copy** from the Edit pull-down menu in the SECURITY MANAGER window, place your cursor in the text input field in which you want to paste the cut text, and select **Paste** from the Edit pull-down menu in the SECURITY MANAGER window. The pasted text will appear in the text input field. To use the Delete option, use the mouse to highlight the text you want to delete, select **Delete** from the Edit pull-down menu and the deleted text will disappear.

3.1.4 Options Menu

The Option menu contains options to determine whether a user account will be local, remote, or global. The Local Accounts option is used to create or modify a user account on the user's workstation. The Remote Accounts option is not currently operable. When this option is enabled, it will be used to give a user access to a local user account on one workstation from a second workstation. The Global Accounts option is used to create or modify a user account for all workstations in the NIS/NIS+ domain. The Global Accounts option cannot be used unless a workstation is configured for NIS/NIS+ and it is important that only the secman is allowed to create global users and profiles.

3.2 Selecting Scope

The current scope of the Security Manager session is displayed on the title bar of all Security Manager windows, as [LOCAL] or [GLOBAL]. The default scope when Security Manager is started on the workstation is local. To change the scope, select the **Options** menu from the main menu bar. It has three options, Local Accounts, Remote Accounts and Global Accounts. Remote Accounts is currently disabled. When either Local or Global Accounts is selected, all scope-sensitive dialogs will be closed (if open), and the Main window will be re-loaded with user account information according to the scope selected.

Changing the scope changes the source of the information available to Security Manager as follows:

When Scope Is Local:

User Accounts:	*/etc/passwd*
Unix Groups:	*/etc/group*
User Directories:	*/h/USERS/local*
Profile Database:	*/h/USERS/local/Profiles*.

When Scope Is Global:

User Accounts:	NIS or NIS+ passwd database
Unix Groups:	NIS or NIS+ group database
User Directories:	*/h/USERS/global*
Profile Database:	*/h/USERS/global/Profiles*.

The selected scope will remain in effect during the session until another scope is selected. Exiting and restarting Security Manager will reset the scope to local.

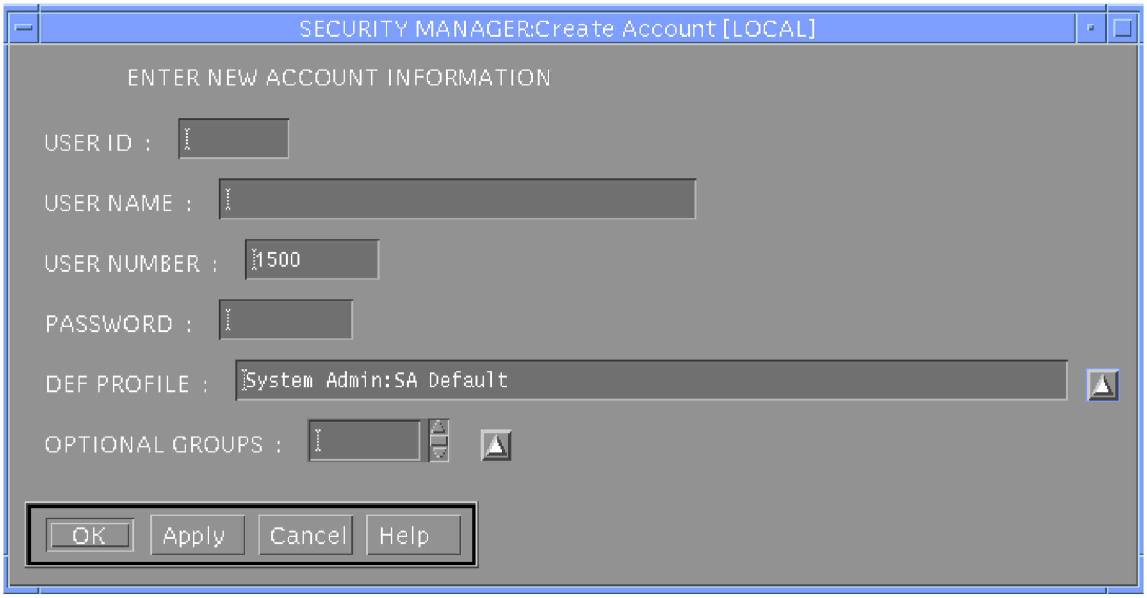
The Global Accounts option will be available based on the configuration of NIS or NIS+ on the system. Global Accounts will be disabled on a standalone workstation. On a NIS client, Global Accounts will be available for viewing, but modifying the accounts or groups is not allowed. On a NIS or NIS+ server, or a NIS+ client added to the administration group, full global account functionality is available.

3.3 Accounts

An account must be established for each user. The user may then be assigned to one or more groups and one or more profiles.

3.3.1 Creating Accounts

To create a user account, select the **Create Account** option from the File menu of Security Manager. If the Create Account option is disabled, Security Manager does not have the ability to create an account for the current selected scope. Otherwise, the Create Account window is presented (see Figure 3-2).



SECURITY MANAGER:Create Account [LOCAL]

ENTER NEW ACCOUNT INFORMATION

USER ID :

USER NAME :

USER NUMBER : 1500

PASSWORD :

DEF PROFILE : System Admin:SA Default

OPTIONAL GROUPS :

Figure 3-2. Create Account Dialog Window

The Create Account window contains the following fields:

User ID: 8 character alphanumeric field for the user login name.

User Name: 40 character field for the name of the account holder.

User Number: An integer field containing the user ID number of the new account. This field defaults to the next highest available number in the range appropriate to the account scope.

Password: 10 character field for the account's login password. Typed text is not shown in the field.

Def Profile: Default profile for the account. This field displays the default profile defined in secman_defaults for the current scope. All profiles defined for the scope are listed in the pop-up list available via the pop-up selection list button to the right of the field. Selecting a profile from the pop-up list will load it into the Def Profile field.

Optional Groups: Scrolled list containing any optional Unix groups that are assigned to the account. A list of all Unix groups for the scope selected is available via the pop-up list button to the right of the field. One or more groups may be selected from the pop-up list and loaded into the Optional Groups field. All optional groups assigned to an account appear listed with the account in the main window of Security Manager.

Follow the steps below to create an account:

Step 1: Select the **Create Account** option from the File pull-down menu. The SECURITY MANAGER: Create Account dialog box appears (see Figure 3-2). A system-assigned user number will appear in the USER NUMBER field.

Step 2: Enter a user name in the USER ID field.

Step 3: Enter a description of the user name in the USER NAME field. The user name must have 40 characters or less.

Step 4: Enter a password in the PASSWORD field. The password must have 10 characters or less.

Step 5: Select a default profile in the DEF PROFILE field. If you click on the DEF PROFILE toggle, the SECURITY MANAGER:DEF (default) window appears. The SECURITY MANAGER:DEF window allows you to select one of the profiles listed.

NOTE: On a new system installation there are only two default profiles to choose from: Security Admin:SSO Default and System Admin:SA Default. The Security Admin:SSO Default profile provides access to all security application menus and options, and the System Admin:SA Default profile provides access to all system application menus and options. <u>Neither of these are to be assigned to users other than the ISSO and the SA</u>.

The profiles that the general users will need must be created before the user accounts can be built. Select a profile by highlighting it and click the **Apply** button to apply your changes. Then click the **OK** button to exit the window.

Step 6: Click on the **OPTIONAL GROUPS** toggle if you want to select optional groups. The SECURITY MANAGER:OPTIONAL window appears. The SECURITY MANAGER:OPTIONAL window allows you to choose one group to which the new user will belong. Select a group by highlighting it and then click the **Apply** button to apply your changes. Then click the **OK** button to exit the window.

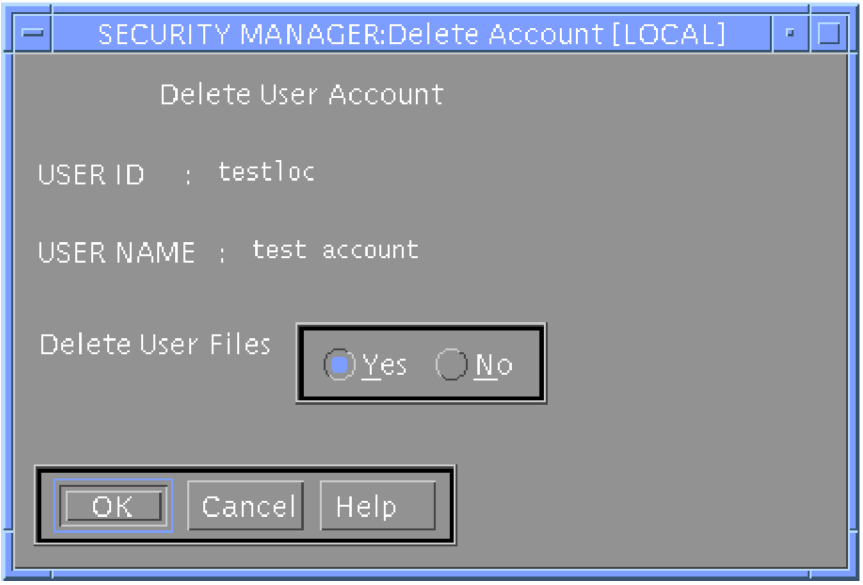
Step 7: Click the **Apply** button in the SECURITY MANAGER:Create Account window to apply your changes. Then click the **OK** button to exit the window. The newly created account will now appear in the SECURITY MANAGER window. See Paragraph 3.3.4 to add additional groups to a users account.

Only the Optional Groups field may be left blank. Once the account is created it will be displayed in the main window of Security Manager. If there is an error creating the account and it is displayed in the main window, delete the account, correct the conditions which caused the error, and re-create the account.

3.3.2 Deleting Accounts

The Delete Account option from the File menu of Security Manager must be enabled to delete an account. If the Delete Account option is disabled, Security Manager does not have the ability to delete accounts for the current selected scope.

First, select the account to be deleted in the main window of Security Manager. It will become highlighted by a single mouse click on the row in the list. Then select the **Delete Account** option from the File menu. A dialog will be presented listing the account to be deleted, and an option to preserve the home directory of the account (see Figure 3-3). The default is to delete the directory, and all files within it. Selecting **OK** from this dialog will delete the account with no further confirmation.



SECURITY MANAGER:Delete Account [LOCAL]

Delete User Account

USER ID : testloc

USER NAME : test account

Delete User Files ● Yes ○ No

Figure 3-3. Delete Account Dialog Window

NOTE:	If preserving the account directory and files, move them to a safe location out of the */h/USERS* structure. If another account is created with the same login name and scope, it will overwrite the existing directory with a blank user account directory structure.

3.4 Groups

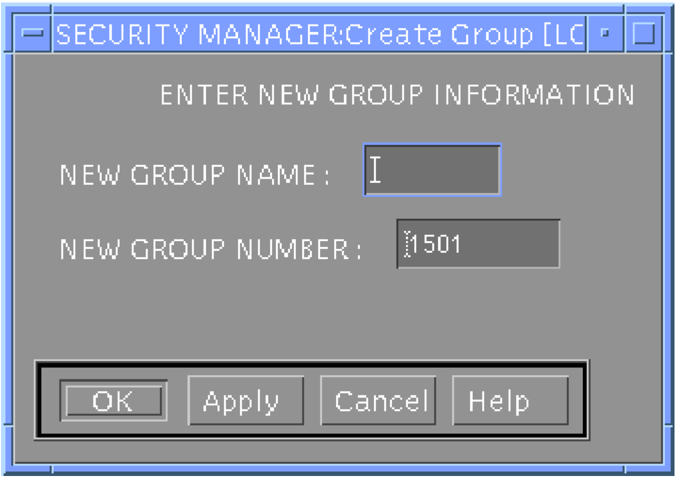
All functions to work with Unix groups are available from the Groups sub-menu from the File menu of Security Manager. If the Groups sub-menu is disabled, Security Manager does not have the ability to alter group information for the current selected scope.

3.4.1 Creating Groups

To create a new Unix group, select the **New** option from the Groups sub-menu. This presents a dialog with two fields for creating a group (see Figure 3-4). The fields are:

New Group Name: 8 character alphanumeric field for the name of the group.
New Group Number: Integer field for the group ID number.

Both fields are mandatory and are checked against existing group names and numbers.



SECURITY MANAGER:Create Group [LC

ENTER NEW GROUP INFORMATION

NEW GROUP NAME :

NEW GROUP NUMBER : 1501

Figure 3-4. New Group Dialog Window

More than one group may share the same numeric group number, but must have unique group names. The logical listing of group ownership is based on group names, but actual file and directory access by group permissions is derived from the group ID number.

3.4.2 Changing Group Names

To change the name of a group, but not the numeric ID of the group, select the **Change** option from the Group sub-menu. This presents a dialog with two fields for changing the Group name (see Figure 3-5). The fields are:

Current Group Name: 8 character alphanumeric field for the name of the group to be changed. It has a pop-up selection list button to the right which will present a list of all Unix groups in the selected scope.

New Group Name: 8 character alphanumeric field for the new name of the group.

Both fields are mandatory and are checked against existing group names.

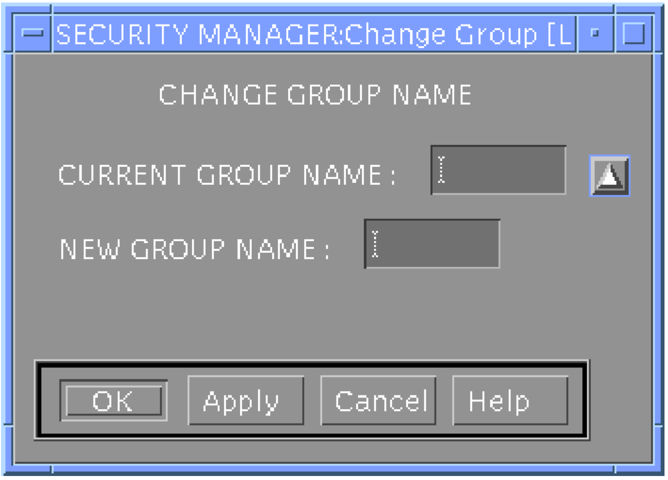


Figure 3-5. Change Group Dialog Window

3.4.3 Deleting Groups

To delete a group from the system, select the **Delete** option from the Group sub-menu. This presents a dialog with one field with a pop-up selection list to select the name of the group to delete (see Figure 3-6). The selected group will be deleted with no further confirmation when the **OK** button is pressed from the Delete Group dialog.

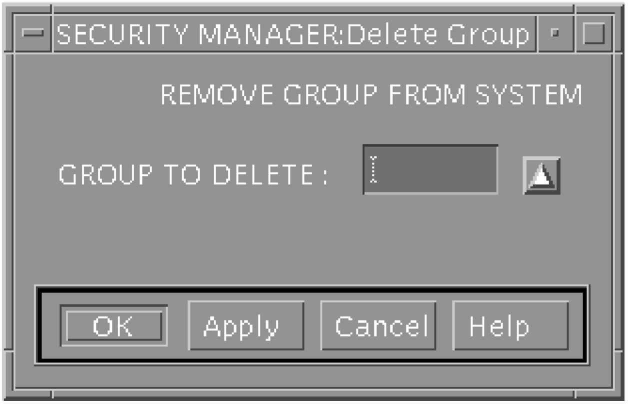


Figure 3-6. Delete Group Dialog

3.4.4 Editing Users and Groups

Security Manager provides a mechanism to manipulate the user accounts assigned to Unix groups in the *group* file, or the NIS group table. This does not alter the default group assigned to the account, which is defined by the default account group and profile.

To change the list of groups to which a user belongs, select the **Edit User's Groups** option from the Groups sub-menu. This presents a dialog with a field which contains a user name and two lists, one for groups assigned to the user and one for groups that are defined but not assigned to the user (see Figure 3-7).

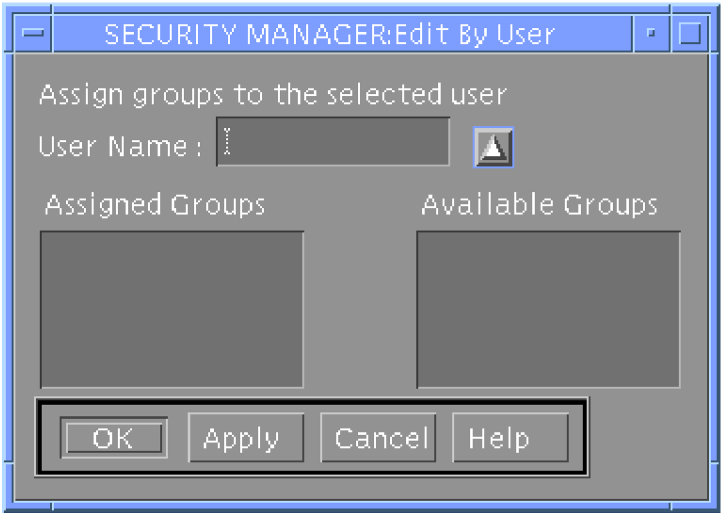

SECURITY MANAGER:Edit By User
Assign groups to the selected user
User Name :
Assigned Groups
Available Groups
OK
Apply
Cancel
Help

Figure 3-7. Edit User's Groups Dialog

Select the desired user from the pop-up selection list to the right of the User Name field. Once a user has been selected, the Assigned Groups and Available Groups lists will be populated based on the current group membership of the selected user. Clicking on a group name in either group list will cause it to be transferred to the other. Once the desired set of assigned groups is reached, press the **OK** or **APPLY** button at the bottom of the dialog to save the changes.

To change the list of users assigned to a group, select the **Edit Group's Users** option from the Groups sub-menu. This presents a dialog with a field which contains a group name and two lists, one for users who are assigned to the group and one for users that exist but are not currently members of the group (see Figure 3-8).

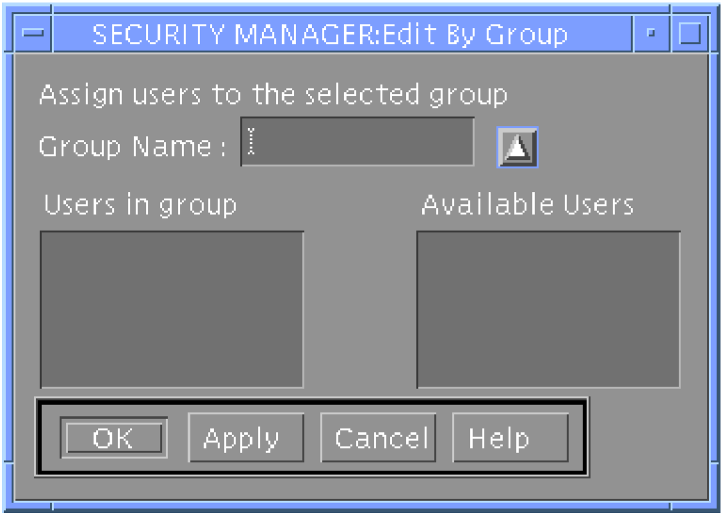

SECURITY MANAGER:Edit By Group
Assign users to the selected group
Group Name :
Users in group
Available Users
OK
Apply
Cancel
Help

Figure 3-8. Edit Group's Users Dialog

Select the desired group name from the pop-up selection list to the right of the Group Name field. Once a group has been selected, the Users in Group list and Available Users list will be populated based on the current membership of the selected group. Clicking on a user name in either list will cause it to be transferred to the other. Once the desired set of assigned users is reached, press the **OK** or **APPLY** button at the bottom of the dialog to save the changes.

3.5 Profiles

Security Manager maintains the user profile database. User profiles are used to restrict user access to data and applications based on their functional needs.

3.5.1 Profile Configuration

The Profile Configuration icon is located in the Application Manager, SSO_Default window and has four options:

1) Profile Selector On/Off: This function determines whether or not the profile selector will be available to a user after successful login. It only applies to users with multiple profiles and has no effect if Profile Locking is turned on.

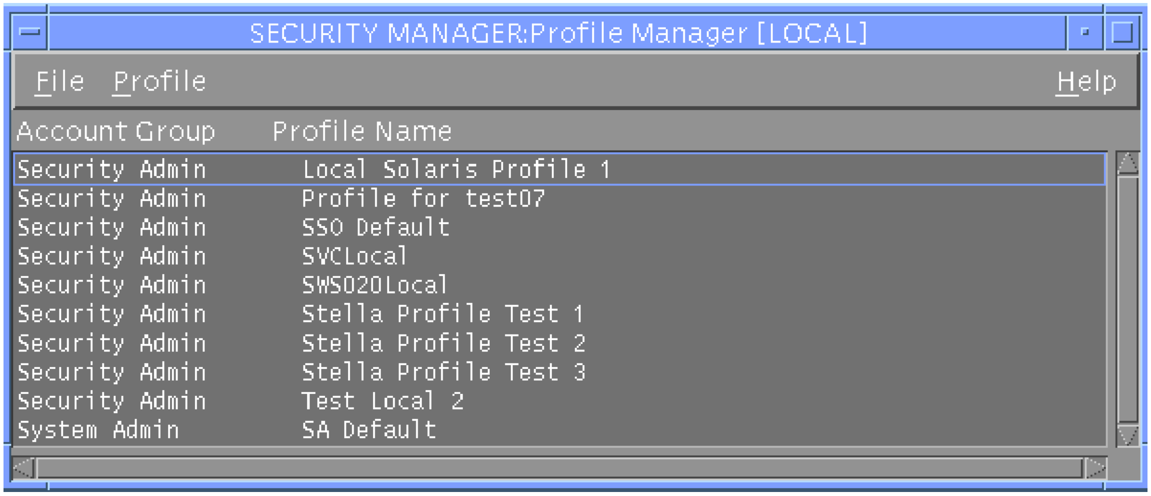
2) Profile Locking On/Off: This toggle allows the SA to restrict the occupancy of a profile to one user at a time within an administrative domain.

3) Profile Auditing On/Off: Turning Auditing On will cause a record to be written to the audit log when a user selects or de-selects a profile.

4) Profile Selection Criteria: This option allows the SA to configure the number of profile selections a user may choose at one time. The choices are either 1 or N, where N is the total number of valid profiles assigned to the user.

3.5.2 Profile Manager Window

To bring up the Profile Manager window, select the **Profiles** option from the File menu on the Security Manager main window. The Profile Manager window is presented (see Figure 3-9). The Profile Manager window contains its own menu bar and a scrolled list in the main area. The scrolled list contains all currently defined profiles by account group for the selected scope.



Account Group	Profile Name
Security Admin	Local Solaris Profile 1
Security Admin	Profile for test07
Security Admin	SSO Default
Security Admin	SVCLocal
Security Admin	SWS020Local
Security Admin	Stella Profile Test 1
Security Admin	Stella Profile Test 2
Security Admin	Stella Profile Test 3
Security Admin	Test Local 2
System Admin	SA Default

Figure 3-9. Profile Manager Window

3.5.3 Creating Profiles

To create a profile, select the **Add Profile** option from the Profile menu on the Profile Manager window. This presents the Add Profile dialog (see Figure 3-10). It contains two fields:

Profile Name: Forty character field for the new profile name.

Account Group: Twenty-five character field for the account group to which the profile belongs. A pop-up selection list button to the right of the field presents a list of all account groups. Selecting an account group from the list will load it into the field.

The new profile will appear in the main list in the Profile Manager window, listed alphabetically by account group, then profile name within the account group.

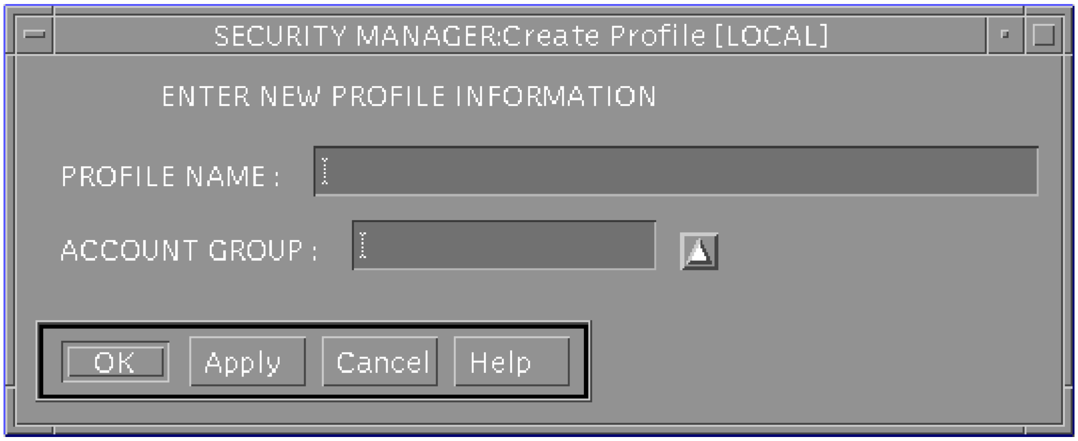
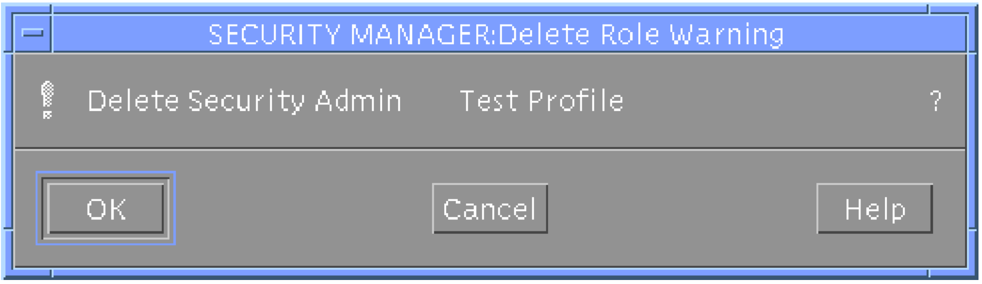

SECURITY MANAGER:Create Profile [LOCAL]
ENTER NEW PROFILE INFORMATION
PROFILE NAME :
ACCOUNT GROUP :
OK
Apply
Cancel
Help

Figure 3-10. Add Profile Dialog Window

3.5.4 Deleting Profiles

To delete a profile, first select the profile in the Profile Manager main window list. This will enable the Delete option in the Profile menu. Select the **Delete** option from the Profile menu. This presents a dialog requiring confirmation to delete the selected profile (see Figure 3-11). If OK is selected, the profile will be deleted with no further confirmation.

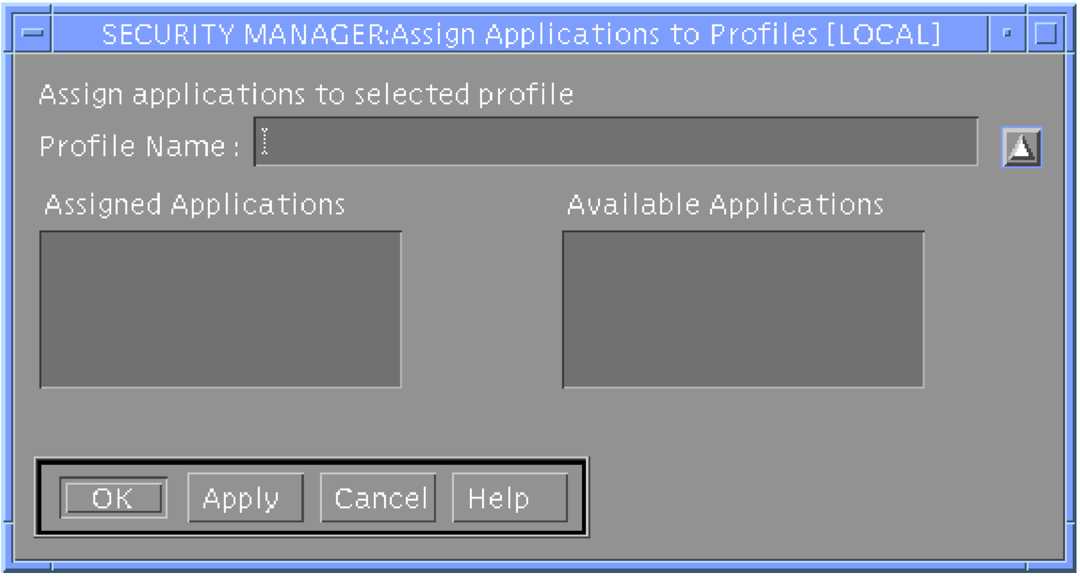

SECURITY MANAGER:Delete Role Warning

Delete Security Admin Test Profile ?

Figure 3-11. Delete Profile Dialog Box

3.5.5 Assigning Applications to Profiles

To assign applications to profiles, select the **Assign Applications** option from the Profile menu on the Profile Manager window. This presents a dialog with a field for a profile name, a list containing applications assigned to a profile, and a list containing defined, but unassigned, applications which are associated with the profile's account group (see Figure 3-12).


SECURITY MANAGER:Assign Applications to Profiles [LOCAL]

Assign applications to selected profile

Profile Name :

Figure 3-12. Assign Applications Dialog Window

Select the desired profile by clicking on the pop-up selection list button to the right of the Profile Name field. This presents all profiles defined for the selected scope. Once the profile is selected, the Assigned Applications and Available Applications lists are populated with application names according to the current state. Click on an application name in one list to transfer it to the other. When the desired set of assigned applications is reached, press the **OK** or **APPLY** button to save the changes. Applications assigned to a profile will appear as icons in the Application Manager window inside the profile's folder.

3.5.6 Assigning Users to Profiles

To assign users to profiles, select the **Assign To User** option from the Profile menu on the Profile Manager window. This presents a dialog with a field for a user name, a list for profiles assigned to the user, and a list for defined profiles that have not been assigned to the user (see Figure 3-13).

NOTE:	In the current release, local users can only be assigned to local profiles. Similarly, global users can only be assigned to global profiles.

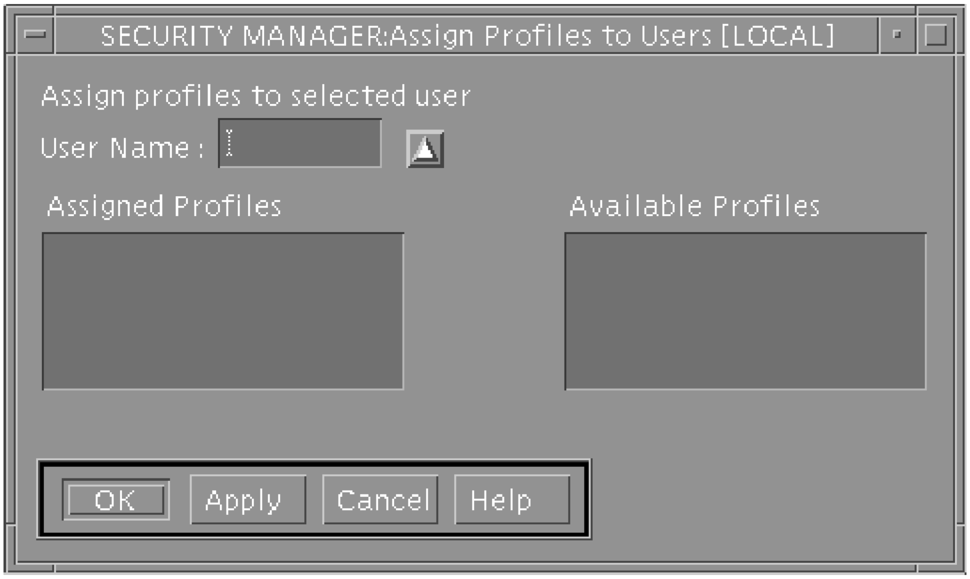

SECURITY MANAGER:Assign Profiles to Users [LOCAL]
Assign profiles to selected user
User Name :
Assigned Profiles
Available Profiles
OK
Apply
Cancel
Help

Figure 3-13. Assign Users to Profiles Dialog Window

Select the desired user by clicking on the pop-up selection list button to the right of the User Name field. This presents all users which have been entered into the profile database in the current selected scope. Once the user is selected, the Assigned Profiles and Available Profiles lists are populated with profile names based on their current assignment to the user. Click on a **profile name** in one list to transfer it to the other. When the desired profiles have been assigned, press the **OK** or **APPLY** button to save the changes.

Profiles assigned to users are available for the user in the Profile Selector. Selected profiles appear as folders within the Application Manager window and are also available for selection using the Profile Selector.

4. Edit Profile Information

4.1 Starting Edit Profiles

Only those user accounts which are assigned to profiles under the Security Admin account group may run Edit Profiles. Follow the steps below to access DII COE security administration functionality:

Step 1: Login as secman.

Step 2: Enter the appropriate password.

Step 3: Double-click on the **Application Manager** icon on the CDE Main Control Panel. Refer to Section 5 of the *DII COE System Administrator's Guide (HP and Solaris)* for more information about CDE.

Step 4: Double-click on the **DII_APPS** icon. The Application Manager - DII_APPS window appears.

Step 5: Double-click on the **SSO_Default** icon. The Application Manager - SSO_Default window appears. This window displays a list of all user accounts.

Step 6: Double-click on the **Edit Profiles** icon. The USER PROFILES window appears.

4.2 User Profiles Window

The USER PROFILES window has four columns: "Profile Name", " Acct Group", "Classification", and "Scope". Each row in the window represents a profile., with its corresponding value of Account Group (" Acct Group"), Classification, and Scope. See Section 3.5 for the Security Manager procedure to create a profile and associate it with an account group.

The USER PROFILES window has three buttons: Edit, Print, and Exit. The process of editing a profile is discussed in Subsection 4.3, and the process of printing the information for a profile is discussed in Subsection 4.4. Exit closes Edit Profiles.

4.3 Editing a Profile

To edit a profile, select the profile in the USER PROFILES window, and press the **Edit** button. This presents the EDIT PROFILE dialog, which has three parts. The top part, PROFILE, displays the Name, Acct Group, and Scope of the selected profile. The middle part, PERMISSIONS, displays the list of permission sets available to the profile. Editing the permissions in these sets is discussed in paragraph 4.3.1. The bottom part, MENU ACCESS, displays the list of menus available to the profile. Editing menu access is discussed in paragraph 4.3.2. When completed editing the permission sets and menu access for the profile, press **OK** to exit the EDIT PROFILE dialog and return to the USER PROFILES window.

4.3.1 Editing Permissions

To edit a set of permissions, select the permission set in the middle part of the EDIT PROFILE dialog, and press the **Edit** button. This presents the EDIT PERMISSIONS dialog. This dialog identifies the selected permission set, and lists the permissions applicable to the set, with an option box for each. Selecting a box will grant the profile the corresponding permission, and deselecting a box will revoke the corresponding permission. When the desired configuration of permissions is reached, press the **OK** to return to the EDIT PROFILE dialog.

4.3.2 Editing Menu Access

To edit access to a menu, select the menu in the lower portion of the EDIT PROFILE dialog, and press the **Edit** button. This presents the EDIT MENU ACCESS dialog. This dialog lists the available menus, with an option box for each. A triangle is also present for each submenu to a listed menu. Selecting a triangle will expand the list to include the corresponding submenu and its contents. Selecting a box will grant the profile access to the corresponding menu or submenu, and deselecting a box will revoke access to the menu. When the desired configuration of menu access is reached, press the **OK** to return to the EDIT PROFILE dialog.

4.4 Printing a Profile

To print a profile, select the profile in the USER PROFILES window, and press the **Print** button.

This page intentionally left blank.